

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

ELLIOTT BROIDY AND
BROIDY CAPITAL MANAGEMENT, LLC,

Plaintiffs,

-v.-

GLOBAL RISK ADVISORS LLC,
KEVIN CHALKER,
DENIS MANDICH,
and ANTONIO GARCIA,

Defendants.

Case No. 1:19-CV-11861

**ANSWER TO SECOND
AMENDED COMPLAINT**

Defendants Global Risk Advisors LLC (“GRA”), Kevin Chalker (“Chalker”), Denis Mandich (“Mandich”), and Antonio Garcia (“Garcia”) (collectively, “Defendants”) by and through their attorneys, Hughes Hubbard and Reed LLP, hereby answer the Second Amended Complaint (the “SAC”) in this action as set forth below.

ANSWER

1. Broidy is a prominent business and civic leader and a philanthropist who has actively served in leadership roles in the Republican Party and Jewish organizations. His advocacy against terrorism and extremism in protection of his country is well known, as is his criticism of Qatar for sponsoring terrorists. Plaintiffs are victims of a hack-and-smear operation whose goal was to silence Broidy’s criticism of Qatar’s support for terrorism. Defendants sought to achieve this objective through the use of computer hacking and surveillance that occurred on numerous occasions in 2017, 2018, and at least the first half of 2019.

ANSWER: Defendants deny the allegations contained in Paragraph 1 that are directed at them, and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in that paragraph.*

2. The hackers were extremely sophisticated and undertook measures to conceal their identities, including through their use of virtual private networks (“VPNs”).

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 2, except that they deny any involvement in the referenced hacking.

3. Nevertheless, through direct and circumstantial evidence, including information provided by third-party sources with direct and personal knowledge of relevant facts (e.g. part D below), and after a diligent inquiry, Plaintiffs have an informed belief that Defendants are responsible for the unauthorized access and theft of Plaintiff’s legally protected electronic communications and other materials.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations about Plaintiffs’ alleged diligent inquiry or information purportedly received from third-party sources, but otherwise deny the allegations that they had any involvement in any alleged access or theft of Plaintiffs’ communications and other materials.

4. Indeed, Plaintiffs have interviewed numerous former GRA employees who have tied Chalker and GRA directly to the hacking, surveillance, and other covert projects for Qatar. The declaration of one of these former GRA employees, made under penalty of perjury, is

* Each Defendant answers each allegation in this complaint separately. Accordingly, where an answer states “Defendants deny,” “Defendants admit,” “Defendants state,” “Defendants refer” (or any similar formulation), that is the case as to each Defendant separately and individually.

attached here and is incorporated into the pleading.

ANSWER: As to the first sentence of Paragraph 4, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of whether and whom Plaintiffs purportedly interviewed and what those unidentified persons allegedly told Plaintiffs, but deny any connection between Defendants and any hacking, surveillance, and other covert projects for Qatar. As to the second sentence of Paragraph 4, Defendants admit that Plaintiffs purport to attach and incorporate a declaration which they describe as set forth in Paragraph 4. Insofar as that declaration is incorporated here, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of paragraphs 1-4 of the declaration; are not required to respond to paragraph 5 of the declaration because it states a legal conclusion; and deny the remaining allegations contained in the declaration.

5. Plaintiffs bring this action to recover damages owed to them under the federal statutes prohibiting computer hacking, theft of trade secrets, and racketeering, as well as related claims arising under California statutory and common law.

ANSWER: Insofar as Paragraph 5 states legal conclusions, no response is required. Defendants aver that pursuant to this Court's Opinion and Order Granting in Part and Denying in Part Defendants' Motion to Dismiss, dated September 26, 2023 (ECF 200) (the "Motion to Dismiss Order"), certain claims, including those related to theft of trade secrets and racketeering, have been dismissed, and no response is required to any allegation in Paragraph 5 related to those claims. As to any remaining allegations, Defendants admit that Plaintiffs purport to seek certain damages under certain claims that they set forth in Paragraph 5, but deny they are liable for any alleged damages in this action.

PARTIES

6. Broidy is a California citizen and the chief executive officer, chairman, and sole member of BCM.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 6.

7. BCM is a venture capital investment company organized under Delaware law and headquartered in California. Because Broidy is BCM's sole member, BCM is a citizen of California.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 7.

8. GRA is a cybersecurity company organized under Delaware law and headquartered in New York. Because Chalker is GRA's sole member, GRA is a citizen of New York.

ANSWER: Defendants admit the allegations contained in the first sentence of Paragraph 8. The allegations contained in the second sentence of Paragraph 8 are legal conclusions to which no response is required.

9. Chalker is the owner and sole member of GRA, which he operates and controls. Chalker is a citizen, resident, and domiciliary of New York. Chalker also owns and/or controls several other affiliated entities, including but not limited to GRA Maven, GRA Quantum, GRA EMEA, GRA Research, Qrypt, Bernoulli Limited, and Toccum Limited. At all relevant times, all of these entities and their employees and agents operated under the direct control and domination of GRA and Chalker.

ANSWER: The allegations in Paragraph 9 concerning control, citizenship, residence, domicile and domination are legal conclusions to which no response is required.

Defendants Chalker and GRA admit that Chalker is an owner and a member of GRA, is involved in the operation of GRA and is an owner of GRA Maven, GRA Quantum, GRA EMEA, GRA Research, Qrypt, Bernoulli Limited, and Toccum Limited. Defendants Mandich and Garcia admit that Chalker is involved in the operation of GRA and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of allegations concerning the ownership of GRA and the other entities mentioned. Defendants lack knowledge or information sufficient to form a belief as to the truth or falsity of allegations concerning “other” unnamed “affiliated entities.” Defendants deny the remaining allegations contained in Paragraph 9.

10. Mandich was the mastermind behind the GRA’s secretive covert operations. At all relevant times, Mandich was acting within the scope of his employment and under Chalker’s direct control.

ANSWER: Defendants deny the allegations contained in Paragraph 10.

11. At all relevant times, Garcia was GRA’s Chief Security Officer and was acting within the scope of his employment and under Chalker’s direct control.

ANSWER: Defendants deny the allegations contained in Paragraph 11.

12. Courtney Chalker is Chalker’s brother and carried out the destruction of electronic devices and other materials containing evidence of the hacking on behalf of GRA and under Kevin Chalker’s direct control.

ANSWER: Pursuant to the Motion to Dismiss Order, Courtney Chalker is no longer a party to this action. Insofar as Plaintiffs direct the allegations in Paragraph 12 at Courtney Chalker, no response is required. Insofar as the allegations in Paragraph 12 are directed at

Defendants, Defendants admit that Courtney Chalker is Kevin Chalker's brother and deny all remaining allegations in that paragraph.

JURISDICTION AND VENUE

13. The Court has diversity jurisdiction under 28 U.S.C. § 1332(a), because Plaintiffs are California citizens whereas Defendants are not. Additionally, the amount in controversy far exceeds \$75,000.

ANSWER: Paragraph 13 contains legal conclusions to which no response is required.

14. The Court also has federal question jurisdiction under 28 U.S.C. § 1331, because this action arises under the laws of the United States.

ANSWER: Paragraph 14 contains legal conclusions to which no response is required.

15. The Court has supplemental jurisdiction under 28 U.S.C. § 1367(a), because Plaintiffs' state law claims are so related to the federal claims that they form part of the same case or controversy.

ANSWER: Paragraph 15 contains legal conclusions to which no response is required.

16. The Court has original jurisdiction under 18 U.S.C. § 1836(c).

ANSWER: Paragraph 16 contains legal conclusions to which no response is required.

17. The Court has personal jurisdiction over GRA because it is headquartered in New York, and thus resides in and is domiciled in this state.

ANSWER: Defendants admit that GRA is headquartered in New York, but the remaining allegations in Paragraph 17 contain legal conclusions to which no response is required.

18. The Court has personal jurisdiction over Chalker because he resides in and is domiciled in New York.

ANSWER: Paragraph 18 contains legal conclusions to which no response is required.

19. Because GRA and Chalker are New York residents, this Court has personal

jurisdiction over the remaining Defendants under 18 U.S.C. § 1965.

ANSWER: Paragraph 19 contains legal conclusions to which no response is required.

20. Also, because the remaining Defendants were acting as agents of GRA and Chalker, the Court has personal jurisdiction under New York CPLR § 302(a)(1).

ANSWER: Paragraph 20 contains legal conclusions to which no response is required.

21. This Court is the proper venue under 28 U.S.C. § 1391(b)(2) and (3), because a substantial part of the events giving rise to Plaintiffs' claims occurred in this district, and at least one Defendant resides in this district.

ANSWER: Paragraph 21 contains legal conclusions to which no response is required.

22. This Court is the proper venue under 18 U.S.C. § 1965(a).

ANSWER: Paragraph 22 contains legal conclusions to which no response is required.

FACTUAL BACKGROUND

A. At the Time the Hack-and Smear Operation Began in 2017, Qatar Had a Motive to Silence Broidy Because of His Increased Criticism of Qatar's Support for Terrorism.

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

23. Elliott Broidy is a staunch supporter of Israel and a recognized leader in conservative Jewish political circles. He has a long history of investing personal time and resources in anti-terrorist causes.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 23.

24. Broidy served on the Department of Homeland Security's Advisory Council between 2006 and 2009. There, he contributed to the report of the Council's Future of Terrorism

Task Force, which called for the elimination of terrorist safe havens throughout the world. Broidy has long provided major funding for the Joint Regional Intelligence Center (“JRIC”), which is a cooperative effort between U.S. federal, state, and local law enforcement agencies to collect, analyze, and disseminate terrorism-related threat intelligence. The JRIC continues to serve as the Regional Threat Assessment Center for the Central District of California. Although Broidy is a committed Republican, his contributions in the area of counter-terrorism and America’s national security have been widespread and bipartisan, including his efforts via the America Matters Foundation, American Freedom Alliance, the George Washington University Center for Homeland Security, the Hudson Institute, the Manhattan Institute of New York, the Pacific Council on International Policy, and the Panetta Institute for Public Policy.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 24.

25. As part of those efforts, Broidy has been an outspoken critic and opponent of the State of Qatar because of the country’s ties to terrorism. Broidy’s efforts to shed light on Qatar’s support for terrorism and its influencing of U.S. foreign policy to be less harsh toward Iran and terrorist groups like Hamas have included, among other things, financial support for think tanks and other non-profits, correspondence with elected and governmental officials, and op-eds in national publications. The Department of Justice has “impaneled a grand jury in Washington, DC. [as part of an] ongoing probe into Qatar’s influence efforts by unregistered operatives,”¹ and in recent months, DOJ has demanded that multiple Qatari-controlled entities must register under

1. <https://www.motherjones.com/politics/2021/04/businessman-charged-with-foreign-lobbying-crimes-paid-for-secret-trump-white-house-mission-to-qatar/>

FARA, including Al Jazeera² and the Qatar-America Institute.³ Neither Chalker nor any of his GRA entities has registered under FARA for representation of Qatar.

ANSWER: Defendants admit on information and belief that Broidy has publicly expressed criticism of the State of Qatar, but state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in the first two sentences of Paragraph 25. The allegations contained in the third sentence of Paragraph 25 refer to certain articles and a press release, and Defendants refer to those for their content. As to the last sentence of Paragraph 25, Defendants admit that Defendants Chalker and GRA have not registered under FARA for representation of Qatar because they have not engaged in any activity requiring such registration.

26. Qatar is widely recognized as a sanctuary for terrorist leaders and organizations, including but not limited to Al Qaeda (including Al-Shabab and Al Qaeda in Syria, also known as Al-Nursa Front or Jabhat Al-Nursa), Hamas, the Taliban, and the Muslim Brotherhood. Indeed, the U.S. Department of Treasury has sanctioned numerous individuals residing in Qatar for raising funds for Al Qaeda. Qatar also has permitted Hamas leaders to operate freely within Qatar and has provided substantial funding to the group, despite the threat of international political and economic sanctions for such support. Similarly, Qatar has allowed the Taliban to operate and maintain an office in Doha since at least 2014. Qatar has given safe haven to many leaders of the Muslim Brotherhood after their expulsion from Egypt by the Egyptian government. And Qatar has allied itself in close strategic partnership with regimes governing

2. <https://www.axios.com/doj-enforce-al-jazeera-foreign-agent-ruling-a5a58129-5a12-4aee-8a2b-cbfb7d8f900.html>

3. <https://www.rubio.senate.gov/public/index.cfm/2020/8/rubio-and-zeldin-lead-members-of-congress-in-urging-aljazeera-s-registration-under-fara>

Iran and Russia.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 26.

27. Broidy has for years viewed Qatar as a major threat to U.S. Security. He has funded public initiatives, such as conferences, to educate Americans about Qatar's support for terrorism.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 27.

28. Broidy's efforts were particularly prominent in 2017. On May 23, 2017, the Foundation for Defense of Democracies ("FDD") hosted a conference entitled "Qatar and the Muslim Brotherhood's Global Affiliates: New U.S. Administration Considers New Policies."

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 28.

29. The speakers at the conference repeatedly argued that Qatar was a state-sponsor of terrorism and that the U.S. should undertake efforts to combat it. For example, Jake Sullivan (the current National Security Advisor) stated that, "we are not placing a high enough priority on the national security threats to the United States that is [sic] emanating from the financing of terror groups by Qatar and other countries. And we have to be doing more on that."

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 29.

30. Broidy partly financed the FDD's conference.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 30.

31. Five months later, on October 23, 2017, the Hudson Institute hosted a similar conference entitled “Countering Violent Extremism: Qatar, Iran, and the Muslim Brotherhood.”

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 31.

32. Like the speakers at the FDD’s conference earlier in the year, the speakers at the Hudson Institute’s conference strongly condemned Qatar’s sponsorship of terrorism and argued for policy changes.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 32.

33. Broidy partially financed the Hudson Institute’s conference.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 33.

34. Broidy also supported President Trump’s 2016 political campaign, and once Trump took office in January 2017, Broidy continued voicing his strong concerns about Qatar at the highest levels of the U.S. government.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 34.

35. Around the same time, President Trump, with whom Broidy had discussed Qatar, criticized the country as “a funder of terrorism at a very high level” and made comments in support of an embargo. President Trump also publicly denounced Qatar through a tweet and during a Republican National Committee meeting in 2017.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 35.

36. During that same month, Qatar's Middle Eastern neighbors were equally unnerved by Qatar's support for terrorist organizations. Saudi Arabia, the UAE, Egypt, Bahrain, and Yemen announced that they were cutting off diplomatic relations with Qatar, and blocking all land, air, and sea travel to and from Qatar.⁴

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in the first sentence of Paragraph 36. The allegations contained in the second sentence of Paragraph 36 purportedly refer to a N.Y. Times article. Defendants refer to that article for its content, except admit on information and belief that in or around 2017, certain Middle Eastern countries cut ties with Qatar.

37. One of Qatar's top D.C. lobbyists, Nicolas Muzin, had also identified Broidy to the Qatari Embassy as an impediment to Qatar's foreign policy interests in the United States. Muzin has signed FARA filings on behalf of his company, Stonington Strategies LLC, which is a registered foreign agent of Qatar. Plaintiffs sued Muzin separately in the U.S. District Court for the District of Columbia, captioned *Broidy Capital Management, et al. v. Nicholas D. Muzin, et al*, No. 1:19-cv-0150 (DLF). Muzin's motion to dismiss in that litigation was denied in part by the district court, and the case is currently on appeal in the D.C. Circuit Court of Appeals.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in the first and second sentences of Paragraph 37. Defendants admit on information and belief the allegations contained in the third sentence of Paragraph 37. The fourth sentence of Paragraph 37 purportedly

4. Anne Barnard & David D. Kirkpatrick, *5 Arab Nations Move to Isolate Qatar, Putting the U.S. in a Bind*, N.Y. Times (June 5, 2017), <https://www.nytimes.com/2017/06/05/world/middleeast/qatar-saudi-arabia-egypt-bahrainunited-arab-emirates.html>

refers to a decision of the U.S. District Court for the District of Columbia in another case and the status of that case on appeal. Defendants refer to that decision and docket for their content.

38. In light of all this, Qatar viewed Broidy as a serious threat to its international standing and, more specifically, to its relationship with the U.S., both of which Qatar feared could ultimately result in the tiny emirate losing some or all of its hosting privileges for the 2022 World Cup. Qatar therefore had a strong incentive to silence Broidy, so as to prevent further criticism and what it considered to be unfavorable changes to U.S. policy.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 38.

B. To Help Neutralize the Threat, Qatar Reached Out to Its Longtime Business Associate, Kevin Chalker.

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

39. As a result of the above, Qatar had motive to neutralize a powerful and high-profile U.S. businessman in Broidy. But it needed to do so in a clandestine and covert manner to maintain deniability and avoid any official connection to the misconduct.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 39.

40. Qatar, Chalker, and GRA had, at the time, an existing business relationship related to denigrating Qatar's critics in order to enhance the wealthy emirate's image and standing in the U.S. and elsewhere more generally. According to former GRA personnel, these denigration campaigns were executed in large part by utilizing tradecraft and other clandestine

skills that Chalker and various GRA employees acquired while working for the CIA or other arms of the U.S. government.

ANSWER: Defendants deny the allegations contained in the first sentence of Paragraph 40. As to the second sentence of Paragraph 40, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs, but deny the substance of what was allegedly told.

41. Indeed, Chalker, through GRA and its affiliated entities, had received tens of millions of dollars for such work.

ANSWER: Defendants deny the allegations contained in Paragraph 41.

42. As a result, GRA was perfectly suited to be engaged by Qatar in an effort to discredit and silence Broidy, thereby neutralizing the effect of his criticisms of Qatar.

ANSWER: Defendants deny the allegations contained in Paragraph 42.

- i. **GRA markets its cybersecurity skills as though it is a legitimate consulting firm, even though it only made money through its “special projects” for Qatar.**

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

43. GRA’s website says that the company provides “the highest caliber of security products and advisory services to governments and multinational corporations worldwide.”

ANSWER: Defendants admit the allegations contained in Paragraph 43.

44. Chalker describes his company as “an international strategic consultancy specializing in cybersecurity, military and law enforcement training, and intelligence-based advisory services.”

ANSWER: Paragraph 44 purports to quote Defendant Chalker, but provides no citation for Defendants to verify whether he is accurately quoted. Defendants admit that Defendant GRA has used the quoted language in describing its services.

45. Despite marketing itself as a consultant and government contractor, GRA's only meaningful revenue came from so-called "special projects" for the State of Qatar, according to former GRA employees.

ANSWER: Defendants admit that GRA markets itself as a consultant and government contractor. Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs, but Defendants GRA and Chalker deny the substance of what was allegedly told and Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what was allegedly told.

- ii. **GRA's personnel are hand-picked from the special ops and intelligence communities and are more than capable of covert hacking.**

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

46. GRA is comprised of former intelligence, national security and military personnel trained in all levels of deception, disinformation, and cyber warfare.

ANSWER: Defendants deny the allegations contained in Paragraph 46.

47. Founded and led by Chalker, a former CIA officer, GRA specifically employs experienced hackers from the intelligence and military communities.

ANSWER: Defendants admit that Defendant Chalker is a former CIA officer who founded and leads GRA, and deny the remaining allegations contained in Paragraph 47.

48. For example, former GRA employee John Sabin was identified by the *New York Times* two months before the start of the hack of Plaintiffs as “a former hacker for the National Security Agency,”⁵ and was also described as “now a director of network security at GRA Quantum.”

ANSWER: Insofar as Paragraph 48 purports to offer an “example” of the allegations contained in Paragraph 47, Defendants refer to, and incorporate here, their response to Paragraph 47. The remaining allegations contained in Paragraph 48 purportedly refer to a N.Y. Times article. Defendants refer to that article for its content. As to footnote 5, Defendants admit that, for a period of time, Roy Wilson had the title of “Managing Director” and was based out of London at that time; [REDACTED FOR REVIEW BY CIA AND DOD]; and deny any remaining allegations with regard to Mr. Wilson in that footnote. Defendants admit that Will Rankin was GRA’s Managing Director of its Washington, D.C. office for a period of time and formerly worked for the CIA, but lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations concerning Mr. Rankin.

49. That same October 2017 article ended with the implication that Sabin himself had actually already managed to circumvent some of the most advanced commercially available encryption technology, including for Gmail: “When asked if he had already circumvented physical multifactor authentication devices like Google’s keys, Sabin would offer only: ‘No comment.’”

5. See Brian X. Chen & Nicole Perloth, How Google’s Physical Keys Will Protect Your Password, N.Y. Times (Oct. 25, 2018), <https://www.nytimes.com/2017/10/25/technology/personaltech/google-keys-advanced-protectionprogram.html>. In addition, GRA’s Managing Director of its London office, Roy Wilson, is a former covert officer in the CIA’s clandestine service, and its former Managing Director of its Washington, DC office, Will Rankin, is a former top CIA expert on illicit finance.

ANSWER: The allegations contained in Paragraph 49 purportedly refer to a N.Y. Times article. Defendants refer to that article for its content.

50. GRA and its associates are experts in the tactical collection of hard-to-access information.

ANSWER: The allegations contained in Paragraph 50 are vague insofar as they refer to “the tactical collection of hard-to-access information.” Accordingly, Defendants deny the allegations in that paragraph.

51. Indeed, GRA holds two patents related to resonant cryptography—a system Chalker co-invented as a method for the secure transmission of data across any network. The patent applications are premised on Chalker’s hacking expertise. Chalker’s own filings showcase his deep understanding of system vulnerabilities to “brute force attack” (cracking a password or other security feature by automated, trial-and-error mechanisms) and argues in one application that it is a “profound understatement” to say that “the current security architecture is woefully inadequate.”⁶ That filing further explains that “[c]omplex systems break and are compromised in complex ways rarely understood or appreciated by their naïve makers. The essence of modern day hacking is based on this principle and only grows with technical complexity”⁷

ANSWER: Defendants admit that GRA held two patents as described in the first sentence of Paragraph 51, except deny that GRA currently holds the referenced patents.

Defendants deny the allegations contained in the second sentence of Paragraph 51.

6. US Patent No. 9,660,803, col. 2 ll. 63-67, col. 3 ll. 60-62 (issued May 23, 2017).

7. *Id.* at col. 3 ll. 3-7.

Defendants deny the allegations concerning Defendant Chalker’s alleged “deep understanding of system vulnerabilities to ‘brute force attack.’” The remaining allegations contained in Paragraph 51 purportedly refer to the patents cited in footnotes 6 and 7.

Defendants refer to those patents for their content.

52. Chalker’s patent argues that no current system is safe from well-funded hackers:

The battle to make devices/hardware/software perfectly secure has already been lost. The signature based tools of firewalls and antivirus software have failed because they cannot predict the future profile of infections. . . . **[I]f your company is a priority target entity at all costs, say by a determined and well-funded state actor, escalating resources will be deployed to break into the network normally reserved for the hardest targets.**⁸

ANSWER: The allegations contained in Paragraph 52 purportedly refer to the patents cited in footnotes 6–8. Defendants refer to those patents for their content.

53. And GRA makes no secret of its ability to use this expertise offensively to penetrate computer networks. GRA has advertised on its website its expertise with “penetration testing,” which refers to hacking into a network to identify its security weaknesses. The underlying skills for penetration testing can be employed offensively or defensively. If an entity has hired an outside consultant to help identify its weaknesses, it is considered a “white hat” operation that is being used defensively to help that entity shore up its security system. But if the entity did not grant that consultant permission to conduct “penetration testing” on its network, and the consultant penetrates the network anyway, it is the same skillset being used in a wholly different, and illegal, type of operation, commonly referred to as a “grey hat” or “black hat” operation.

8. *Id.* at col. 4 ll. 6-22 (emphasis added).

ANSWER: Defendants deny the allegations contained in the first sentence of Paragraph 53. As to the second sentence, Defendants purportedly refer to GRA's website, and Defendants refers to that website for its content, and deny all remaining allegations in that sentence. Defendants GRA, Mandich and Garcia deny the allegations contained in the third, fourth and fifth sentences of Paragraph 53 as vague and fundamentally misleading. Defendant Chalker states that he lacks knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in those sentences.

54. GRA's current website highlights case studies involving "penetration testing" and "pioneering military training."

ANSWER: The allegations contained in Paragraph 54 purportedly refer to GRA's website. Defendants refer to that website for its content.

55. In October 2015, GRA's website more explicitly marketed "Grey Hat + Penetration Testing" that described GRA's expertise in the exact sort of hacking techniques employed against Broidy and BCM:

GRA's Grey Hat + Pen Testing (GHPT) service is a comprehensive suite designed to evaluate an organization's perimeter, public, and private network security. We utilize advanced techniques developed from years of expertise within the US government and private sector. These experiences include penetrating the networks of America's adversaries, such as, terrorists and narcotics organizations.⁹

ANSWER: The allegations contained in Paragraph 55 purportedly refer to GRA's website as of 2015. Defendants refer to that website for its content.

56. And in a 2015 video promoting GRA's Grey Hat service, GRA admits to having

9. <http://web.archive.org/web/20151002155106/http://globalriskadvisors.com/>;
<http://web.archive.org/web/20150830070535/http://www.globalriskadvisors.com/wp-content/uploads/Global-Risk-Advisors-Grey-Hat-Penetration-Testing.pdf>

“advanced techniques to penetrate target networks,” including private sector, private networks.¹⁰

The video states that GRA employs both common attack methods to intrude into servers and, also, “uncommon and customized attacks,” including custom “spear phishing” campaigns.

ANSWER: The allegations contained in Paragraph 56 purportedly refer to a video. Defendants refer to that video for its content.

57. Mandich, a former CIA officer, worked for GRA and under Chalker’s direct control at all relevant times. According to former GRA personnel, Mandich’s job duties included designing the “special projects” at the direction of Chalker.

ANSWER: The allegations contained in the first sentence of Paragraph 57 concerning control are legal conclusions to which no response is required. As to the remaining allegations contained in that sentence, Defendants admit that Mandich is a former CIA officer who worked for GRA for a certain period of time, and deny the remaining allegations in that sentence. As to the second sentence of Paragraph 57, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs, but Defendants GRA, Chalker and Mandich deny the substance of what was allegedly told and Defendant Garcia states that he lacks knowledge or information sufficient to form a belief as to the truth or falsity of what was allegedly told.

58. Garcia, a former U.S. Marine, worked as GRA’s chief information officer and under Chalker’s direct control at all relevant times. According to former GRA personnel, Garcia assisted Chalker by destroying evidence, including electronic devices, of the Broidy hacking

10. Global Risk Advisors, *GRA GreyHat Penetration Testing Service*, You Tube (Oct. 28, 2015), <https://www.youtube.com/watch?v=BLAYD64JxXQ>

after Broidy initiated litigation.

ANSWER: The allegations contained in the first sentence of Paragraph 58 concerning control are legal conclusions to which no response is required. As to the remaining allegations contained in that sentence, Defendants admit that Garcia is a U.S. Marine Veteran who worked for GRA for a certain period of time, and deny the remaining allegations in that sentence. As to the second sentence of Paragraph 58, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs, but deny the substance of what was allegedly told.

59. Likewise, Courtney Chalker, acting as an agent of GRA and under his brother Kevin Chalker's direct control, destroyed evidence of the Broidy hacking, according to former GRA personnel.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs, but deny the substance of what was allegedly told. Insofar as Plaintiffs direct the allegations contained in Paragraph 59 at Courtney Chalker, no response is required because, pursuant to the Motion to Dismiss Order, Courtney Chalker is no longer a party to this action.

60. While GRA had hackers in a number of locations, many of the GRA hackers working on this campaign were located in GRA Research's offices in Northern Virginia. GRA broadly employed many former intelligence and Special Forces personnel with offensive hacking and surveillance skills developed while in government service, with a large team in Northern Virginia that was referred to as the "Reston Group" and affiliated with GRA Research. The Reston Group was centrally involved in many "special projects" hacking and surveillance

operations, including the hack-and-smear operation targeting Plaintiffs.

ANSWER: Defendants deny the allegations contained in Paragraph 60.

61. The head of the Reston Group was a former CIA official with information security expertise. Other members in the Reston Group included a software engineer formerly with the military, a former member of the Army's special operations forces, and others with prior work experience in cyberwarfare and employing disinformation in furtherance of campaigns to denigrate targeted entities. The Reston Group included one particularly trusted operative, Defendant Anthony Garcia, who was GRA's Chief Security Officer.

ANSWER: Defendants deny the allegations contained in Paragraph 61.

iii. **Chalker leveraged his history with Qatar and the skills of his employees into a lucrative business relationship.**

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

62. Chalker's relationship with Qatar dated back to his time in the CIA, according to former GRA personnel.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs, but Defendant Chalker [REDACTED FOR REVIEW BY CIA AND DOD]; and the remaining Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegation that Defendant Chalker's work for the CIA involved Qatar.

63. Qatari official Ali al-Thawadi, known as "Shep," is the Chief of Staff to the Qatari Emir's brother, and has long been GRA's primary contact. Shep worked with GRA on

the World Cup special projects. GRA frequently provided updates to Shep regarding surveillance activities, including of American citizens.

ANSWER: Defendants GRA and Chalker admit the allegations contained in the first sentence of Paragraph 63 and deny the remaining allegations in that paragraph.

Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the first two sentences of Paragraph 63 and deny the allegations contained in the third sentence of that paragraph.

64. According to former GRA personnel, when Abdullah Al-Thawadi (a high-ranking Qatari official) was abducted for ransom in or around 2009, his sons turned to Chalker for assistance. Chalker frequently bragged to employees and non-employees that he successfully obtained Al-Thawadi's release, thereby earning the trust of Qatari officials.

ANSWER: As to the first sentence of Paragraph 64, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs; Defendant Chalker denies the substance of what was allegedly told; and the remaining Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what was allegedly told. Defendants deny the allegations contained in the second sentence of Paragraph 64.

65. According to former GRA personnel, Qatar subsequently engaged GRA to assist Qatar in its efforts to secure the bid for the World Cup 2022. This and similar work were referred to as "special projects." GRA's efforts were ultimately successful, as Qatar was awarded the World Cup bid and has managed to retain it since then, despite strong criticism that was eventually silenced.

ANSWER: As to the first sentence of Paragraph 65, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs, but deny the substance of what was allegedly told. Defendants GRA and Chalker deny the allegations contained in the second sentence of Paragraph 65, and Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in that sentence. Defendants deny the allegations contained in the third sentence of Paragraph 65.

66. For years, GRA worked to help Qatar win its blatantly corrupt bid for the 2022 World Cup and then to maintain it, even when the bid was on the verge of being revoked because of growing concern with Qatar's unsavory conduct, including the use of slave labor for construction.

ANSWER: Defendants deny the allegations contained in Paragraph 66.

67. For example, a widely-covered report by Amnesty International documented slave-like labor conditions in Qatar's construction sector where workers went without pay for months on end (or sometimes without pay at all), had their passports confiscated so they could not leave the country, and were forced to live in "squalid" accommodations.¹¹

ANSWER: The allegations contained in Paragraph 67 purportedly refer to an Amnesty International report. Defendants refer to that report for its contents, and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegation that the report was "widely-covered."

11. Amnesty International, *The Dark Side of Migration: Spotlight on Qatar's Construction Sector Ahead of the World Cup* (Nov. 18, 2013), <https://www.amnesty.org/download/Documents/16000/mde220102013en.pdf>

68. In connection with that bid, Qatar has been credibly accused of bribery on a massive scale, offering to pay hundreds of millions of dollars to FIFA officials to secure hosting privileges.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or the falsity of the allegations contained in Paragraph 68.

69. Qatar's corrupt bid eventually led to the convictions or guilty pleas of over sixteen individuals,¹² and the criminal investigation is not yet over—a superseding indictment outlining additional bribery charges was filed as recently as April 2020.¹³

ANSWER: The allegations contained in Paragraph 69 purportedly refer to a U.S. Department of Justice Press Release and an indictment. Defendants refer to those documents for their content.

70. Indeed, the younger brother of the Qatari Emir, Sheikh Mohamad bin Hamad Al Thani, known as “MBH,” told third parties that Qatar was indebted to Chalker for the work he had done on the World Cup.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 70.

71. Given the prior successes of GRA and Chalker in its covert work for Qatar, it only made sense that Qatar would approach Chalker about silencing Broidy when Broidy's criticism of Qatar peaked in 2017.

ANSWER: Defendants deny the allegations contained in Paragraph 71.

12. Press Release, U.S. Dep't of Justice, *Sixteen Additional FIFA Officials Indicted for Racketeering Conspiracy and Corruption* (Dec. 3, 2015), <https://www.justice.gov/opa/pr/sixteen-additional-fifa-officials-indicted-racketeeringconspiracy-and-corruption>.

13. *See United States v. Webb, et al.*, No. 1:15-CR-00252 (E.D.N.Y.) (Apr. 6, 2020 Superseding Indictment).

72. At the time it won the World Cup hosting rights in 2010, and during the years that followed, Qatar’s successful bid was met with enormous controversy, highlighting its precarious standing in the worldwide soccer community—a community that had never before voted to allow a Middle Eastern nation to host its premier event. Holding on to the 2022 World Cup—and the tremendous economic and reputational boost that goes along with it—was a matter of desperate national urgency.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 72.

73. In August 2012, a formal inquiry was launched to investigate Qatar’s corrupt winning bid two years earlier by the International Federation of Association Football (“FIFA”), which is the global body governing competitive soccer, including the World Cup.

ANSWER: Defendants admit on information and belief the description of FIFA included in Paragraph 73. Defendants admit on information and belief that, at some point in time, FIFA launched an investigation into the bidding process for the 2022 World Cup, but state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in Paragraph 73.

74. The investigation FIFA launched in 2012 documented extensive corruption, including bribery and astroturfing, utilized by Qatar to win the 2010 bid for the 2022 World Cup, and it was detailed in a 353-page report, known publicly as the “Garcia Report,” based on the name of the lead investigator, former U.S. Attorney Michael J. Garcia. Even though the Garcia Report was submitted to FIFA in or around November 2014, it was not released to the public until a German news outlet in June 2017 published a leaked copy of the PDF of the full report.

ANSWER: Defendants admit on information and belief that, at some point in time, FIFA launched an investigation into the bidding process for the 2022 World Cup. Insofar as the allegations contained in Paragraph 74 purportedly refer to a report by former U.S. Attorney Michael J. Garcia (the “Garcia Report”), Defendants refer to that report for its content, and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in Paragraph 74.

75. GRA was paid handsomely by Qatar for their work supporting the corrupt World Cup 2022 Bid.

ANSWER: Defendants deny the allegations contained in Paragraph 75.

76. GRA’s work for Qatar grew to expand beyond the World Cup. GRA was retained in part to target Qatar’s political enemies through cyber operations and public relations, to protect Qatar’s geopolitical interests. According to former GRA personnel, Qatar retained GRA to execute these larger-scale programs on its behalf and entered into consultancy arrangements with GRA worth at least \$100 million, primarily for covert conduct.

ANSWER: Defendants deny the allegations contained in the first and second sentences of Paragraph 76. As to the third sentence of Paragraph 76, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs, but deny the substance of what was allegedly told.

77. GRA’s covert cyber operations for Qatar involved a pattern of attacks against political targets involving similar fake news alerts, malicious Google login pages, email addresses designed to mimic legitimate Google security addresses, falsified two-factor authentication messages, and the use of Mail.ru to control victims’ accounts.

ANSWER: Defendants deny the allegations contained in Paragraph 77.

78. As has been publicly reported in *The New York Times* and other media outlets, forensic evidence indicates that Qatar, and therefore GRA, were likely involved in targeting over 1,000 people and entities via cyberattacks similar to those deployed against Plaintiffs here, including prominent officials from countries like Egypt and the UAE, and the United States, including an American political columnist and activist, Rabbi Shmuley Boteach, all of whom are known as outspoken critics of Qatar.¹⁴

ANSWER: The allegations contained in Paragraph 78 purportedly refer to articles in the N.Y. Times and other outlets. Defendants refer to those articles for their contents. Insofar as the allegations contained in Paragraph 78 are directed at Defendants, Defendants deny those allegations.

79. One of the targeting projects was highly successful and has particular salience here: GRA's hacking and surveillance of the UAE Ambassador to the United States. In or around April and May 2017, approximately a half-year before it attacked Broidy, GRA conducted similar cyberattacks against the UAE Ambassador, who has extensive interactions with politically active Americans in an effort to improve Qatar's image with the United States by not only discrediting him, but also intimidating (and ultimately silencing) U.S. government officials and other Americans who were either critics or potential critics of Qatar.

ANSWER: Defendants deny the allegations contained in Paragraph 79.

80. As with Broidy, hacked emails were disseminated to the media by an anonymous

14. See Shmuley Boteach, "Qatar's War to Destroy Pro-Israel Jews," Jerusalem Post, Oct. 8, 2018, <https://www.jpost.com/Opinion/Qatars-war-to-destroy-pro-Israel-Jews-568942>; Eli Lake, "Russian Hackers Aren't the Only Ones to Worry About," Bloomberg, Sept. 18, 2018, <https://www.bloomberg.com/opinion/articles/2018-0918/russian-hackers-aren-t-the-only-onesto-worry-about>.

“source” identified only by an alias— “GlobalLeaks”—in an effort to embarrass not just the primary target, but also politically active associates, ultimately silencing active critics and preventing others from voicing their own criticisms.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 80.

81. Mandich was the mastermind behind the Global Leaks operation, overseeing the execution of every phase of the operation. On information and belief, John Sabin and Defendants Garcia and Kevin Chalker also worked with Mandich in carrying out the Global Leaks campaign.

ANSWER: Defendants deny the allegations contained in Paragraph 81.

82. In June 2017, *The Huffington Post* wrote one of the first stories under the headline “Someone Is Using These Leaked Emails To Embarrass Washington’s Most Powerful Ambassador.”¹⁵ The article stated that, “In private correspondence, [UAE Ambassador] Otaiba— an extremely, powerful figure in Washington, D.C., who is reportedly in ‘in almost constant phone and email contact’ with Jared Kushner.”

ANSWER: The allegations contained in Paragraph 82 purportedly refer to a Huffington Post article. Defendants refer to that article for its content, and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegation that this article was “one of the first stories” under the referenced headline.

83. Another article, published in *The Intercept*, was titled “Diplomatic Underground:

15. Akbar Shahid Ahmed, Someone Is Using These Leaked Emails To Embarrass Washington’s Most Powerful Ambassador, *The Huffington Post* (June 3, 2017).

The Sordid Double Life of Washington’s Most Powerful Ambassador,”¹⁶ and was clearly designed to embarrass the UAE Ambassador. The article relied on hacked emails, and notes that the emails “began to dribble out just as a geopolitical row between the UAE and its neighbors in Qatar came to a head.”

ANSWER: Insofar as the allegations contained in Paragraph 83 purportedly refer to an article published in The Intercept, Defendants refer to that article for its content, and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in Paragraph 83.

84. An article in *The New York Times*, based on hacked emails was likewise intended to embarrass the UAE. The article states: “Anonymous hackers have provided a long series of leaked emails from Ambassador Yousef al-Otaiba’s Hotmail account to The New York Times and other news organizations over the past two years in an apparent campaign to embarrass the U.A.E. and benefit Qatar.”¹⁷

ANSWER: Insofar as the allegations contained in Paragraph 84 purportedly refer to an article published in N.Y. Times, Defendants refer to that article for its content, and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in Paragraph 84.

85. There are striking similarities to the attack on Elliott Broidy. Both operations relied on producing highly curated and specifically-themed PDFs, which were disseminated to some of the same friendly reporters, including Ryan Grim (*The Intercept*), Bradley Hope (*The*

16. Ryan Grim, Diplomatic Underground: The Sordid Double Life of Washington’s Most Powerful Ambassador, *The Intercept* (Aug. 30, 2017).

17. David D. Kirkpatrick, Persian Gulf Rivals Competed to Host Taliban, Leaked Emails Show, N.Y. Times (July 31, 2017).

Wall Street Journal), and David Kirkpatrick (*The New York Times*), with stories based on hacked materials still being published well over a year after the publication of the first such article.

There are no publicly-known other similar campaigns that disseminated hacked materials via curated, themed PDFs, let alone over many months to those same reporters. Additionally, Howard was among the public relations professionals pitching stories based on the hacked material, just as he would later do with the Broidy hack. And the execution of the two attacks included several tactics in common, such as: (1) use of messages from Gmail accounts that appeared to be official; (2) messages that displayed a correct but redacted phone number for the victim; (3) deployment of evasion tactics to help bypass automatic spam filter and other security alerts; (4) use of private registration services and “throw away accounts” from the Mail.Ru group; and (5) maintenance of multiple phishing sites but hosting them on their own dedicated servers, using different subdomains for different campaigns.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 85.

86. Indeed, the similarities were lost on no one. The BBC quoted an unnamed “source familiar” with the hack as saying that the Broidy attack was “rinse and repeat on Otaiba.”¹⁸

ANSWER: Insofar as the allegations contained in Paragraph 86 purportedly refer to an article published in the BBC, Defendants refer to that article for its content, and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in Paragraph 86.

18. Suzanne Kianpour, Emails show UAE-linked effort against Tillerson (Mar. 5, 2018), <https://www.bbc.com/news/world-us-canada-43281519>

87. Moreover, the UAE Ambassador hack was successful in silencing certain critics of Qatar. For example, the Foundation for the Defense of Democracies (FDD) had consistently criticized Qatar's support for Islamic extremism and terrorism. On May 23, 2017, FDD hosted (with Plaintiffs' involvement) a conference largely focused on exposing Qatar's misdeeds. Less than a week later, after learning that their communications had been intercepted in the UAE Ambassador hack, FDD executive director Mark Dubowitz informed Mr. Broidy that the think tank would no longer publicly criticize the wealthy emirate because they feared potential Qatari reprisal. Two months later, the only FDD scholar whose work had substantially focused on Qatar left the think tank, and no one was hired or reassigned to replace his work relating to Qatar.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 87.

88. GRA's numerous cyberattacks have extended over several years and represent a pattern of unlawfully accessing victims' computer systems to extract private information or other items of value with which to attack or damage the enemies of its clients, typically for the purpose of silencing criticisms of Qatar's support for terrorist groups or its abysmal record on human rights.

ANSWER: Defendants deny the allegations contained in Paragraph 88.

89. In addition to cyberattacks in which information was stolen, Qatar has used unlawful and unauthorized access to computer systems to plant documents that would appear to incriminate their purported enemies.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 89.

90. These cyberattacks are all part of the pattern of racketeering activity in which the Enterprise conspirators have engaged with the common purpose of silencing critics of Qatar.

ANSWER: Defendants deny the allegations contained in Paragraph 90 insofar as those allegations are directed at them, and state that they otherwise lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in that paragraph.

91. GRA's work for Qatar extended well beyond the World Cup. Even though Qatar had gained notoriety in the years following its successful 2010 bid to host the 2022 World Cup as a high-tech "dirty tricks" operator engaged in astroturfing and hacking, Qatar lacked the internal capability to carry out sophisticated hacking and surveillance operations. This void in Qatar's capabilities was why the tiny emirate paid GRA Defendants millions of dollars in and around 2018 to conduct "Operation Deviant," whose primary purpose was teaching members of Qatar's Special Forces and Intelligence services both defensive and *offensive* cybersecurity skills, including advanced, sophisticated skills that trained former U.S. intelligence and military operatives are typically barred from sharing or conferring unto foreign governments. According to former GRA personnel, Chalker and GRA routinely ignored U.S. legal requirements to obtain International Traffic in Arms Regulations (ITAR) and other regulatory approvals, despite the lifetime ban on former CIA agents conferring tradecraft knowledge and skills to foreign governments. Chalker divulged classified information on tradecraft, as well as sensitive equipment and dual-use technology to the Qataris in support of this illicit work. According to former GRA personnel, these disclosures harmed U.S. national security by helping enhance the covert, illicit capabilities of a known supporter of terrorist groups, including al Qaeda and Hezbollah.

ANSWER: Insofar as the allegations contained in Paragraph 91 are “according to former GRA personnel,” Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons allegedly told Plaintiffs; Defendants Mandich and Garcia deny the substance of what was allegedly told, and Defendants Chalker and GRA [REDACTED FOR REVIEW BY CIA AND DOD].

92. In the years immediately following Qatar’s winning World Cup bid, GRA’s role with the wealthy emirate grew to encompass protecting Qatar’s geopolitical interests primarily by planning and executing covert operations to target Qatar’s political enemies through cyber operations and public relations. According to former GRA personnel, Qatar retained GRA to execute these larger-scale programs on its behalf and entered into consultancy arrangements with GRA worth at least \$100 million, primarily for covert conduct.

ANSWER: Defendants deny the allegations contained in the first sentence of Paragraph 92. As to the second sentence of this paragraph, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons allegedly told Plaintiffs, but deny the substance of what was allegedly told.

93. Phone records show that in the weeks leading up to the Broidy hacks, Shep had multiple calls with Joey Allaham—one of the public relations officials who was involved in the media dissemination and use of the Broidy hacked materials.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 93.

94. Tarek Hashem, Shep’s senior adviser, acted as Shep’s “eyes and ears” to ensure the progress of the hack-and-smear campaign and to relay information between GRA and Qatar.

ANSWER: Defendants deny the allegations contained in Paragraph 94.

C. GRA Hacks BCM's Server, Resulting in Thousands of Malicious Connections to Broidy's Email Accounts.

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

95. Beginning in December 2017, Broidy's family and associates began receiving spear phishing emails.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 95.

96. The GRA Defendants first targeted people who were close to Broidy—including his wife and his executive assistant—to obtain their respective log-in credentials to BCM's private server where the confidential documents were stored.

ANSWER: Defendants deny the allegations contained in Paragraph 96.

97. "Spear phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, often for malicious reasons."¹⁹

ANSWER: The allegations contained in Paragraph 97 purportedly refer to a Guardian article. Defendants refer to that article for its content.

98. On December 27, 2017, four spear phishing emails were sent to Broidy's wife, Robin Rosenzweig, and a Broidy Associate. In the following week, Rosenzweig and the Broidy Associate received at least another dozen spear phishing emails.

19. See <https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-andphishing>.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 98.

99. Chalker celebrated the launch of the spear phishing campaign that very night, on Wednesday, December 27, 2017, by taking associates to the Sapphire Gentlemen's club in New York City.

ANSWER: Defendants deny the allegations contained in Paragraph 99.

100. The emails were disguised to appear as though they were Google security alerts, and they asked the Broidy Associate and Rosenzweig to enter their Gmail login credentials into a malicious link embedded in the emails. Unfortunately, Rosenzweig unwittingly complied.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 100.

101. The link in the spear phishing email was designed to appear as if it would direct Ms. Rosenzweig to a legitimate URL on [Google.com](https://www.google.com), but (not readily apparent without viewing the underlying source code) the link was in fact a TinyURL link that directed her to a professionally designed website that was intended to trick victims into believing it was actually an authentic Google account login page. TinyURL is a redirecting service that provides shortened URLs that redirect a website visitor to the website associated with the longer, masked URL. It is known to be used by hackers and scammers to avoid detection and circumvent spam and malware filters. When Rosenzweig clicked the TinyURL link, she was redirected to a website that contained Google's logo and appeared to be an authentic Google account update page—but it was in fact a fraudulent login page.

ANSWER: Defendants GRA, Chalker and Mandich state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained

in Paragraph 101. Defendant Garcia states that he lacks knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in the first and fourth sentences of Paragraph 101, admits that the second sentence of that paragraph provides a reasonable definition of TinyURL. As to the third sentence of Paragraph 101, Mr. Garcia states that he lacks knowledge or information sufficient to form a belief as to whom Plaintiffs are referring and whether it is known by such unidentified people.

102. On or about January 3, 2018, the GRA Defendants used the “Mail.ru” service to access and modify Ms. Rosenzweig’s Gmail account without her consent. “Mail.ru” signifies a Russian email service that publishes an app that can be operated by users physically located around the world, including in the United States, to send and receive emails on Mail.ru or other email services like Gmail. Here, the GRA Defendants used the “Mail.ru” to read, send, delete, and manage emails and other documents in Ms. Rosenzweig’s Gmail account, without her knowledge or consent, which in turn enabled them to obtain her log-in credentials for the BCM server.

ANSWER: Defendants admit on information and belief that “Mail.ru” is a Russian email service and deny all remaining allegations contained in Paragraph 102.

103. Indeed, the GRA Defendants even modified Ms. Rosenzweig’s account settings so as to keep her from discovering that her email had been hacked. They arranged for emails containing “Mail.ru,” “viewed,” or “alert” to be marked as read and moved immediately to her trash folder. The GRA Defendants did this to ensure that any legitimate security alerts would not be viewed by Ms. Rosenzweig. And unbeknownst to Ms. Rosenzweig, on January 4, 2018, she received a true security alert—that went directly to her trash folder—notifying her that a user or users of the Mail.ru app had obtained access to read, send, delete, and manage her Gmail

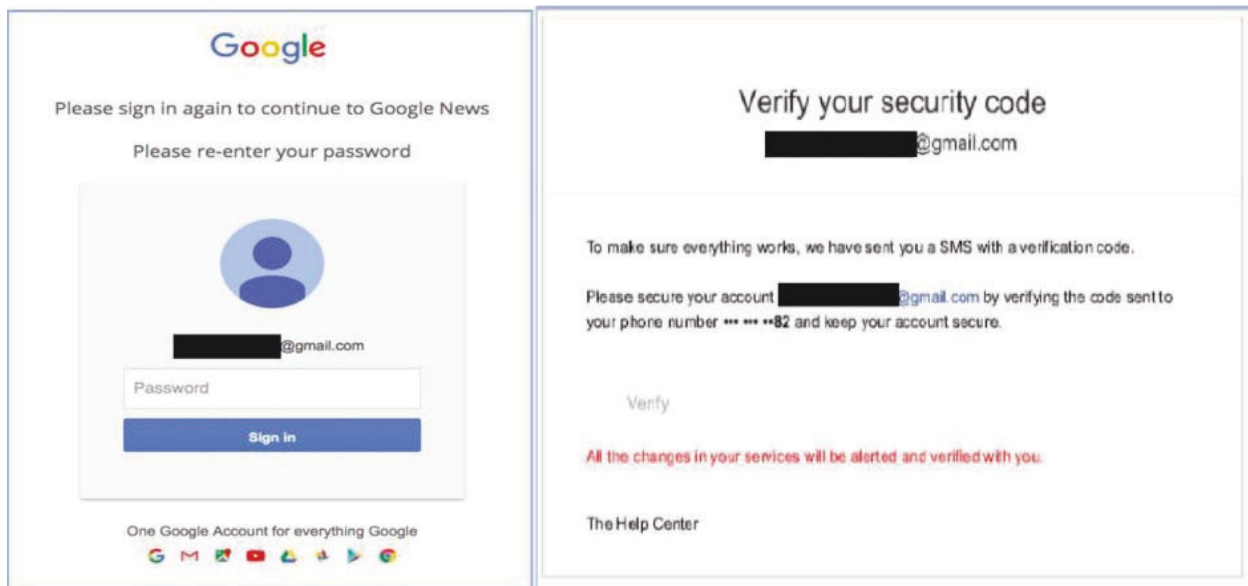
account, all without her awareness or consent.

ANSWER: Defendants deny the allegations contained in the first three sentences of Paragraph 103. Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in the fourth sentence of Paragraph 103.

104. On January 14, 2018, another Broidy associate, Erica Hilliard (“Hilliard”), received two spear phishing emails, which were similarly disguised to look like security alerts from Google. Like her colleagues, Hilliard unwittingly entered her Gmail login credentials, thereby compromising her account.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 104.

105. Examples of the highly sophisticated spear phishing emails are shown below:



ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegation that the screenshots contained in Paragraph 105 are examples of spear phishing emails.

106. Without authorization, Defendants logged into Rosenzweig's Gmail account on January 4, 7, 9, and 17, and they logged into Hilliard's Gmail account on January 14, 15, 16, and 17.

ANSWER: Defendants deny the allegations contained in Paragraph 106.

107. By accessing the Gmail accounts of Rosenzweig and Hilliard, Defendants obtained the login credentials for the Gmail account of another BCM employee, Jenna Pressley Caganap and used those credentials to access Caganap's Gmail account on January 4.

ANSWER: Defendants deny the allegations contained in Paragraph 107.

108. Through the Gmail accounts of Rosenzweig, Hilliard, and/or Caganap, Defendants obtained the login credentials for several BCM email accounts.

ANSWER: Defendants deny the allegations contained in Paragraph 108.

109. On January 16, Defendants accessed the BCM server, without authorization, through the BCM email accounts of Broidy, Caganap, and Hilliard, as well as other BCM employees Michelle Levi, James Sexton, and Jessica Stephens.

ANSWER: Defendants deny the allegations contained in Paragraph 109.

110. BCM has an exchange server physically located in Los Angeles, California, that is connected to the internet and used to engage in commerce and communications throughout the country. The server allows BCM employees to send and receive business and occasional personal emails. Broidy and other employees, including those identified in the preceding paragraph, have secure email accounts on the BCM server containing private communications that require at least a username and password for access.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 110.

111. From January 16 to February 25, 2018, BCM's server was subjected to approximately 325,000 malicious connections from 59 unique internet protocol ("IP") addresses.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 111.

112. Two of these connections were traced to a single IP address in Qatar. Eight of the connections were traced to an IP address belonging to a hotel in Killington, Vermont. Four of the connections were traced to an IP address belonging to an acupuncture business in Wallingford, Vermont.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 112.

113. The remaining hundreds of thousands of connections were disguised by VPNs and are untraceable.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 113.

114. During these attacks, numerous email communications and documents were viewed, stolen, and/or altered without authorization. These included, among other things, Broidy's personal emails and documents, contacts file, business calendar, business emails and documents, signed contracts, attorney-client privileged communications and documents, attorney-client work product, usernames, and passwords to access other non-Google accounts, including email accounts on the computer network of BCM, including Broidy's corporate email account, financial information, and confidential business process and methods information. The server also contained corporate and personal documents, copyrighted material, contracts, business plans, and other confidential and sensitive proprietary information, to which Defendants

had full access.

ANSWER: Defendants deny any allegations contained in Paragraph 114 directed at them and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in that paragraph.

115. Broidy filed a lawsuit shortly after the hacking occurred. The lawsuit triggered a panic within GRA, which was eager to destroy the evidence inculcating it in the hacking scheme. Kevin Chalker instructed GRA's Chief Security Officers, also a GRA Research hacker in the Reston Group, Anthony Garcia, to wipe GRA's computers, phones and other devices clean of any damaging evidence. Garcia not only complied with that instruction, but he removed certain hard drives, phones and devices with incriminating evidence from GRA's offices, and brought them to a remote location, where the devices were destroyed and ultimately discarded. Courtney Chalker knowingly assisted Garcia with the destruction of evidence.

ANSWER: Defendants deny the allegations contained in Paragraph 115.

D. Former GRA Employees and Associates Confirmed That Chalker and GRA Were Responsible for the Hack-and-Smear of Broidy and BCM.

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

116. Chalker told GRA personnel that Chalker and GRA were responsible for the hack-and-smear operation targeting Broidy/BCM.

ANSWER: Defendants deny the allegations contained in Paragraph 116.

117. Chalker also told GRA personnel that Chalker, Garcia, and Courtney Chalker had destroyed electronic devices and other materials containing evidence of the Broidy/BCM hacking as soon as this litigation was filed. This was done to conceal the role of GRA and Kevin

Chalker in the hacking.

ANSWER: Defendants deny the allegations contained in Paragraph 117.

118. In addition to the hacking, Chalker and GRA also directed the electronic and physical surveillance of Broidy, according to former GRA personnel.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons allegedly told Plaintiffs, but deny the substance of what was allegedly told.

119. Attached as Exhibit A is a declaration from a former GRA employee attesting to well-founded knowledge of GRA's involvement in the Broidy / BCM hack-and-smear operation. The declaration is anonymous to protect the security and safety of this whistleblower from retaliation from Defendants. Defendants have a history of threatening former employees. Plaintiffs have also offered to submit to the Court for *in camera* review a copy of the original, signed declaration for the Court to verify the signature and the identity of the declarant. In addition, undersigned counsel have interviewed other former GRA employees and can attest to his credibility as to the statements made in the declaration.

ANSWER: As to the first sentence of Paragraph 119, Defendants admit that Plaintiffs purport to attach, as Exhibit A, a declaration from an unidentified person described as a former GRA employee, but lack knowledge or information sufficient to form a belief as to whether that is true or false, and deny the remaining allegations in that sentence. As to the attached declaration, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of paragraphs 1-4 of the declaration; are not required to respond to paragraph 5 of the declaration because it states a legal conclusion; and deny the remaining allegations contained in the declaration. Defendants deny the

allegations contained in the second and third sentences of Paragraph 119. Defendants admit that in a June 1, 2021 letter to the Court, Plaintiffs stated that they make an “offer to submit for *in camera* review a copy of the original, signed version of the declaration attached as Exhibit A to the [then-]proposed second amended complaint,” and refer to that letter for any details regarding that offer. *See* ECF 98. Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in Paragraph 119, but deny that the purported anonymous declarant has any credibility as to his declaration regarding Defendants.

E. In the Months Leading up to the Hack-and-Smear Operation, Chalker’s Off-Shore Companies Received Massive Payments from Qatar.

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

120. According to information provided by former GRA personnel, Qatar paid Chalker through three off-shore entities, Bernoulli Limited (“Bernoulli”), Toccum Limited (“Toccum”), and GRA EMEA, all of which are based in Gibraltar. This was done to maintain the clandestine nature of the operations and avoid the appearance of any official connection between Qatar and GRA.

ANSWER: As to the first sentence on Paragraph 120, Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs, but Defendants Chalker and GRA admit that Qatar made payments into accounts of the three entities listed in the paragraph, and Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the substance of what was allegedly told.

Defendants Chalker and GRA deny the allegations contained in the second sentence of Paragraph 120, and Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in that sentence.

121. During all relevant times, Chalker owned and controlled Bernoulli, Toccum, and GRA EMEA.

ANSWER: Defendants GRA and Chalker admit that Chalker is an owner of Bernoulli, Toccum, and GRA EMEA. Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the ownership of Bernoulli, Toccum, and GRA EMEA. The remaining allegations contained in Paragraph 121 are legal conclusions to which no response is required.

122. Indeed, the connection between GRA and the three off-shore entities is shown in the New York Department of State's records.

Selected Entity Name: BERNOULLI LIMITED

Selected Entity Status Information

Current Entity Name: BERNOULLI LIMITED

DOS ID #: 5419853

Initial DOS Filing Date: OCTOBER 03, 2018

County: NEW YORK

Jurisdiction: ALL OTHERS

Entity Type: FOREIGN BUSINESS CORPORATION

Current Entity Status: ACTIVE

Selected Entity Address Information

DOS Process (Address to which DOS will mail process if accepted on behalf of the entity)

GLOBAL RISK ADVISORS LLC
ONE WORLD TRADE CENTER
83RD FLOOR
NEW YORK, NEW YORK, 10007

Registered Agent

NONE

Selected Entity Name: TOCCUM LIMITED

Selected Entity Status Information

Current Entity Name: TOCCUM LIMITED

DOS ID #: 5419846

Initial DOS Filing Date: OCTOBER 03, 2018

County: NEW YORK

Jurisdiction: ALL OTHERS

Entity Type: FOREIGN BUSINESS CORPORATION

Current Entity Status: ACTIVE

Selected Entity Address Information

DOS Process (Address to which DOS will mail process if accepted on behalf of the entity)

GLOBAL RISK ADVISORS LLC

ONE WORLD TRADE CENTER

83RD FLOOR

NEW YORK, NEW YORK, 10007

Registered Agent

NONE

Selected Entity Name: GLOBAL RISK ADVISORS EMEA LIMITED

Selected Entity Status Information

Current Entity Name: GLOBAL RISK ADVISORS EMEA LIMITED

DOS ID #: 5455345

Initial DOS Filing Date: DECEMBER 07, 2018

County: NEW YORK

Jurisdiction: ALL OTHERS

Entity Type: FOREIGN BUSINESS CORPORATION

Current Entity Status: ACTIVE

Selected Entity Address Information

DOS Process (Address to which DOS will mail process if accepted on behalf of the entity)

GLOBAL RISK ADVISORS LLC

ONE WORLD TRADE CENTER,

83RD FLOOR

NEW YORK, NEW YORK, 10007

Registered Agent

NONE

ANSWER: The allegations contained in Paragraph 122 purportedly refer to certain New York State records. Defendants refer to those records for their content.

123. The publicly available financial statements for Bernoulli, Toccum, and GRA EMEA further show that they received combined payments approximately totaling at least \$30 million in the months leading up to the launch of the hack-and-smear operation in December

2017.

Bernoulli Limited

Registered Number: 20 November 2017 153

BALANCE SHEET as at 31 December 2017


	31-Dec-17 USD	31-Dec-16 USD
FIXED ASSETS	-	-
CURRENT ASSETS		
Debtors due within one year	1,212,194	8,100,148
Cash at Bank and in Hand	21,156,490 22,368,684	13,586,133 21,686,281

Toccum Limited

Registered Number: 8th March 2019 108685

BALANCE SHEET as at 31 December 2017

	31-Dec-17 USD	31-Dec-16 USD
FIXED ASSETS	-	-
CURRENT ASSETS		
Debtors	45,213	45,473
Cash at Bank and in Hand	18,602,095 18,647,308	29 45,502

Global Risk Advisors EMEA Limited		
		
<div style="display: flex; justify-content: space-between;"> <div>Registered Number: 107892</div> <div style="border: 1px solid red; border-radius: 50%; padding: 5px; text-align: center;"> 8th March 2019 GIBRALTAR * </div> </div>		
BALANCE SHEET as at 31 December 2017		
	31-Dec-17 USD	31-Dec-16 USD
FIXED ASSETS	-	-
CURRENT ASSETS		
Debtors	3,240	28,240
Cash at Bank and in Hand	3,279,323	33
	3,282,563	28,273

ANSWER: Insofar as the allegations contained in Paragraph 123 purportedly refer to certain publicly-filed financial statements, Defendants refer to those for their content, and deny that they were involved in any hack-and-smear operation.

124. According to former GRA personnel, who had knowledge of GRA's finances, this money was paid by Qatar, which was GRA's only meaningful client and source of overseas funds.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told Plaintiffs, but deny the substance of what was allegedly told.

125. Also according to former GRA personnel, GRA held weekly status meetings to track unpaid invoices. The invoices were not related to the work that GRA held itself out as doing for Qatar, i.e. standing up an intel fusion center in Doha. During these same conversations, GRA employees discussed GRA conducting "dark" operations for Qatar.

ANSWER: Insofar as the allegations contained in paragraph 91 are "according to former GRA personnel," Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of what unidentified persons purportedly told

Plaintiffs. Defendants GRA and Chalker [REDACTED FOR REVIEW BY CIA AND DOD]. Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the substance of what was allegedly told, and deny any allegations related to “dark” operations for Qatar.

126. Another GRA employee, Dan Emory, who was also involved in the “special projects,” was responsible for getting the invoices paid by Ali al-Thawadi—the Chief of Staff to MBH, the Qatari Emir’s younger brother.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 126. Defendant Garcia denies that Mr. Emory was a GRA employee and states that he lacks knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in Paragraph 126. Defendant Mandich states that he lacks knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 126.

F. To Complete Their Plan of Silencing Broidy’s Criticisms, Defendants Provided the Hacked Materials to Media Outlets That Published Salacious Stories.

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

127. Qatar’s objective to effectively stifle Broidy’s First Amendment freedoms was not complete until the materials stolen by GRA and Chalker could be twisted and publicized to smear Broidy’s reputation.

ANSWER: Defendants deny the allegations contained in Paragraph 127.

128. Thus, after the hacking was completed and the materials had been stolen from Broidy and BCM, Defendants carefully packaged the hacked materials into a series of PDFs,

each with a unique theme designed to inflict maximum damage through highly precise curation and alteration, then leaked those PDF files to the media, with the help of third parties.

ANSWER: Defendants deny the allegations contained in Paragraph 128.

129. The PR strategist members used by Qatar include, among others, Nicholas Muzin, Joseph Allaham, Gregory Howard, Ahmad Nimeh, BlueFort Public Relations LLC, Spark Digital, Stonington Strategies, and Lexington Strategies.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 129.

130. Through all times relevant to this Second Amended Complaint, Nicolas D. Muzin was the Chief Executive Officer of Stonington Strategies LLC, a public relations and lobbying firm incorporated under the laws of Delaware, and a political lobbyist who signed FARA documents on behalf of Stonington as a registered foreign agent for the State of Qatar. On August 24, 2017, he was officially retained by the State of Qatar for “consulting services,” and on September 3, 2017, Stonington registered under FARA as a foreign agent providing “strategic communications” for the State of Qatar. Stonington Strategies has been reorganized into Stonington Global LLC, whose website states that “[i]n launching the new firm, Nick Muzin & his team plan to build on their success representing the State of Qatar.”

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 130.

131. Joseph Allaham was the co-founder of Stonington Strategies, where he served as partner for all relevant times. He has worked for Qatar, originally as an unregistered foreign agent until he eventually filed a registration statement under FARA on June 15, 2018, in response to a subpoena from Plaintiffs in a related action. He is also the CEO of Lexington

Strategies.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 131.

132. Gregory Howard is a media placement expert, an agent who, through his relationships with members of the media, provides information and materials to the media to generate stories desired by the agent's client. In 2017 and 2018, Howard worked as a Vice President and Senior Media Strategist at the firm of Conover & Gould ("Conover"), based in Washington, DC. From July 2017 until January 18, 2018, Howard was a registered foreign agent of Qatar through Conover, but continued working for months afterwards placing stories in the media based on Broidy's hacked materials, despite terminating his status as a registered agent of Qatar. Beginning no later than May 10, 2018, Howard worked in Washington, DC, as Vice President of Mercury Public Affairs, a public strategy firm, which he left in April 2019. In each of his positions at Mercury, despite FARA filings that did not mention Qatar, Howard worked as a media placement strategist for Qatar.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 132.

133. Qatar specifically retained Messrs. Muzin, Allaham, and Howard in an attempt to influence the Republican, American-Jewish community and other conservative supporters of the President, with the end goal of influencing White House policy. Their work included identifying Broidy and other Americans as critics to be silenced.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 133.

134. Muzin began working for Qatar sometime in 2017, and in late August of that year,

the Qatari Embassy in Washington, DC, officially retained Stonington and Muzin to influence public opinion regarding Qatar. Their agreement specified that Muzin and Stonington were to provide “consulting services” including the “development and implementation of a government relations strategy for Qatar, as requested and directed by the Embassy.” The initial agreement that Muzin submitted to the U.S. Department of Justice provided that Qatar would pay Muzin and Stonington Strategies \$50,000 a month for these services.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 134.

135. The initial agreement further limited Muzin and Stonington Strategies from acting as “a representative, spokesperson or agent on behalf of the Embassy or the State of Qatar in any meeting or communication with any person, or in any public or private statement, or in any communications with the media” “[e]xcept as directed by the Embassy.”

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 135.

136. Allaham also began working for Qatar in 2017, according to his initial FARA disclosures in his capacity as the CEO of Lexington Strategies.²⁰ According to his (subsequently filed) FARA registration, he worked directly for the Emir of Qatar, Sheikh Tamim bin Hamad Al Thani, and his brother Sheikh Mohamad bin Hamad Al Thani (the Emir’s brother is commonly referred to as “MBH”) Allaham’s FARA filing listed MBH’s chief of staff, Ali Al-Thawadi, as his official point of contact responsible for overseeing his work on behalf of Qatar—meaning his supervisor in the chain of command was the same as for the GRA Defendants. GRA worked

20. <https://efile.fara.gov/docs/6563-Registration-Statement-20180615-2.pdf>

with these same individuals and referred to them for purposes of their covert operations by code names.

ANSWER: Defendants deny the allegations contained in Paragraph 136 that are directed at Defendants, except that Defendants GRA and Chalker admit that their primary point of contact in Qatar was Ali Al-Thawadi. Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in Paragraph 136.

137. In the fall of 2017, in the weeks leading up to the attack, phone records show that Allaham had five separate phone calls with MBH's chief of staff, Ali al-Thawadi. GRA also worked very closely with Thawadi and gave him the code name, "Shepherd," or "Shep," for short.

ANSWER: Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 137, except that they admit that GRA worked with "Shep" in connection with the World Cup. Defendants GRA and Chalker state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in the first sentence of Paragraph 137; admit the allegation in the second sentence of Paragraph 137 that they worked closely with Al-Thawadi, also known as "Shepherd," or "Shep," and deny the remaining allegations in that sentence.

138. Also working in fall of 2017 with both GRA and the DC Defendants was Ahmad Nimeh, the person behind "Blue Fort PR," the firm that paid Muzin and Allaham at least \$3.9 million in a span of three weeks from mid-September through early October 2017.

ANSWER: Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 138. Defendants GRA and Chalker deny any allegations contained in Paragraph 138 that are directed at GRA and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in the rest of the paragraph.

139. Nimeh was someone with whom GRA worked closely, to the extent that GRA gave him the code name “Botany.” Nimeh is the principal of a company that worked alongside GRA on the World Cup projects and who was publicly reported to be part of the Qatar “black ops” team hired to undermine rival bidders (including the eventual runner-up, the United States). According to both reporting in the *Sunday Times of London* and someone who has seen Nimeh’s communications from during and around 2010, Nimeh worked with PR agents, as well as Chalker, in furtherance of Qatar’s “dirty tricks” operations—and Nimeh did so under the direct supervision of Ali Al-Thawadi, aka “Shep.”

ANSWER: Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 139. Defendants GRA and Chalker admit that they referred to Nimeh as “Botany;” deny any other allegations contained in Paragraph 139 that are directed at GRA; and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in the rest of the paragraph.

140. On or around September 17, 2017, Chalker met with Shep and Hashem in New York City. Shortly thereafter, Chalker flew to Doha in the first week of October 2017 to have a follow-up meeting with Shep and Hashem. These meetings Chalker had with Shep and Hashem coincided with Blue Fort PR’s two payments of \$1.95 million each to Muzin on September 18

and October 10, 2017, as well as Qatar's payment of \$1.45 million in "October 2017" to Allaham.

ANSWER: Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 140. As to the allegations contained in the first two sentences of Paragraph 140, Defendants GRA and Chalker admit on information and belief that, in or around September 2017, Defendant Chalker met with Shep and Hashem in New York City, deny that Defendant Chalker flew to Doha in the first week of October 2017 to have a follow-up meeting with Shep and Hashem, and aver that Defendant Chalker visited Qatar in or around that time. Defendants GRA and Chalker deny the remaining allegations contained in Paragraph 140 insofar as they are directed at GRA, and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in Paragraph 140.

141. Chalker flew again to Doha to meet with "Shep" and Hashem during the first week of February 2018, right around the halfway point of the hacking phase of the hack-and-smear operation.

ANSWER: Defendants deny the allegations contained in Paragraph 141 related to the "hack-and-smear operation;" Defendants GRA and Chalker admit that Defendant Chalker flew to Doha to meet with Shep and Hashem during the first week of February 2018; and Defendants Mandich and Garcia state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in that paragraph.

142. Muzin has admitted that he identified and described Broidy to the Qatari

government as impediments to Qatar's foreign policy interests in the United States. In connection with his work for Qatar, Muzin or his employees or agents participated in weekly meetings at the Qatari Embassy in Washington, DC, where they discussed with Qatari officials and other Qatari agents the ongoing efforts against Broidy. Muzin specifically mentioned Broidy in these meetings as an obstacle that needed to be dealt with for his lobbying on behalf of Qatar to succeed.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 142.

143. As plans for the upcoming hack were underway, increased payments flowed to these key public relations strategists. On December 15, 2017, shortly before the hacks on Plaintiffs' computers began, Qatar gave a \$500,000 balloon payment to Messrs. Muzin and Allaham's firm, Stonington Strategies, and increased the monthly retainer from \$50,000 to \$300,000.²¹

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 143.

i. Qatari Public Relations Contractors Push Certain Reporters to Publish Damaging Stories Based on Hacked Materials

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

144. Howard's phone calls following the hacking show that he was in close and frequent communication with journalists in the early months of 2018 before those same reporters

21. <https://efile.fara.gov/docs/6458-Exhibit-AB-20171221-2.pdf>

began publishing stories that relied on information stolen from Plaintiffs' computer systems and servers. In some instances, Howard communicated with journalists for weeks before they published these articles. The intensity of those contacts often increased in the days prior to publication. During this same period, Howard closely communicated with public relations experts, research groups, and registered agents of Qatar to coordinate the media disinformation campaign against Broidy.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 144.

145. Starting on January 7, 2018, just hours after the first sustained hacker access of Ms. Rosenzweig's Gmail account (and thus hundreds of Plaintiffs' confidential documents), Howard engaged in a flurry of calls with his then-colleagues at Conover & Gould and outside public relations professionals, as well as exchanging five phone calls with Amb. Patrick Theros, who is Nimeh's father-in-law and business partner. In the half-year before January 7, 2018, Howard's phone records indicate no calls or text messages with Theros.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 145.

146. From January 18 through at least July of 2018, Howard participated in more than two hundred phone calls with reporters who contributed to stories regarding Broidy and Qatar or regularly covered Qatari-related issues. These included extensive, and at times, almost daily calls with now-former Associated Press ("AP") reporter Tom LoBianco, all leading up to the time he authored several stories regarding Broidy in March and May, 2018, based on the contents of Broidy's hacked emails. In addition, in the same time frame, Howard conducted more than 100 calls with the *New York Times*, *McClatchy*, the *Wall Street Journal*, and the

Washington Post, all of which were focusing on stories regarding Broidy's hacked emails.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 146.

147. Messrs. Muzin and Allaham were in close contact with high-ranking members of the Qatari government (including GRA contacts Apex (the Emir), Mightier (MBH, the Emir's brother), and Shep (Al Thawadi) in the weeks leading up to the attack. Muzin then flew to Qatar within a few days of GRA's first successful hack into Plaintiffs' systems. Messrs. Muzin and Allaham's text messages with each other demonstrate their direct and prior knowledge of the hacking and their knowing use of stolen documents.

ANSWER: Defendants admit that GRA had contacts with the Emir, MBH and Al-Thawadi, deny any other allegations contained in Paragraph 147 directed at GRA and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in that paragraph.

148. On January 25, 2018, shortly after GRA's successful hacking of BCM began, Muzin sent Allaham a message on WhatsApp, stating, "It's very good. . . . We got the press going after Broidy. I emailed you."

ANSWER: Defendants deny any allegations contained in Paragraph 148 directed at GRA and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in that paragraph.

149. That same day, prior to the first public reports in the United States of materials stolen from Plaintiffs, Ben Wieder, a reporter for *McClatchy*, a Washington, DC publication focused on politics, emailed Muzin to tell him, "I'm working on a story about Elliott Broidy and was hoping to talk." Muzin, who was still in Qatar, forwarded this message to Allaham and

commented, “Time to rock.” Less than an hour after sending the email to Muzin, Wieder called Howard, and they spoke for more than 10 minutes. Wieder would go on to write extensively about Broidy on the basis of carefully curated emails and other documents stolen from Broidy’s servers.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 149.

150. On March 1, 2018, the contents of emails stolen from Plaintiffs’ computer accounts and servers appeared for the first time in media accounts. The *Wall Street Journal* credited its source as “a cache of emails from Broidy’s and his wife’s email accounts that were provided to the Journal.”

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in the first sentence of Paragraph 150. The second sentence of Paragraph 150 purportedly refers to a Wall Street Journal article. Defendants refer to that article for its content.

151. Muzin shared the *Wall Street Journal* article with Allaham over WhatsApp that same day. Muzin then commented, “He’s finished.”

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 151.

152. Other media outlets continued to publish more of the stolen emails, including the *Huffington Post* on March 2, 2018, and the BBC on March 5, 2018. The Huffington Post cited “[e]mails and documents an anonymous group leaked to HuffPost.”

ANSWER: The allegations contained in Paragraph 152 purportedly refer to a Huffington Post article and the BBC. Defendants refer to those sources for their content, and state

that they lack knowledge of information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in that paragraph.

153. On March 13, 2018, Muzin remarked to Allaham via WhatsApp that recent news stories about Broidy have “[p]ut[] him in [M]ueller[’s] crosshairs.” This communication demonstrates one of the central goals of the Qatari-Funded Criminal Enterprise—to portray Broidy as a target of special counsel Robert Mueller’s investigation.

ANSWER: Defendants deny any allegations contained in Paragraph 153 directed at GRA and state that they lack knowledge or information sufficient to form a belief as to the truth of the remaining allegations contained in that paragraph.

154. That same day, Allaham wrote to Muzin on WhatsApp that a former U.N. official working under contract with the Qatari government, Jamal Benomar, had gone to Qatar prior to the date of the message “to get the emails. That what [*sic*] I think he was doing there [in Qatar].” Muzin responded by referencing Broidy by name.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 154.

155. On March 14, 2018, Muzin told Allaham on WhatsApp that he’d “get some intel about the Broidy event soon.” This comment likely refers to a March 13, 2018, Republican fundraiser headlined by the President of the United States, for which Broidy had been listed as an event host.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 155.

156. The next day, on March 15, 2018, Muzin exclaimed to Allaham, via WhatsApp, “Elliott Broidy was not at the fundraiser!” The two were clearly excited at the prospect of having

damaged Broidy's political standing.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 156.

157. Multiple additional news stories followed that expressly relied on the stolen documents. On March 21, 2018, the *New York Times* published a front-page article noting that an "anonymous group critical of Broidy's advocacy of American foreign policies in the Middle East" has been distributing "documents, which included emails, business proposals and contracts," belonging to Plaintiffs. On March 23, 2018, *Bloomberg* published an article about Broidy, which noted that it had "received two separate documents this week purporting to be versions" of materials belonging to Broidy.

ANSWER: The allegations contained in Paragraph 157 purportedly refer to "multiple additional news stories," including articles from the N.Y. Times and Bloomberg. Defendants refer to those articles for their contents.

158. On March 25, 2018, a front-page story in the *New York Times* reported extensively on Broidy's fundraising and business activities. The story reported that Broidy had agreed not to attend the March 13 fundraiser. The story was based, in part, on "[h]undreds of pages of Broidy's emails, proposals and contracts" received from what the *Times* euphemistically termed "an anonymous group critical of Broidy's advocacy of American foreign policies in the Middle East." This "anonymous group" is the Qatari-Funded Criminal Enterprise.

ANSWER: Defendants deny any allegations contained in Paragraph 158 directed at them. The remaining allegations contained in Paragraph 158 purportedly refer to a N.Y. Times article. Defendants refer to that article for its content.

159. On March 26, 2018, *McClatchy* published a story authored by Ben Wieder that

used hacked materials to denigrate Broidy, House Foreign Affairs Chairman Ed Royce, and the Congressman's wife, Marie Royce—just four days before the Senate was scheduled to vote on her appointment to be Assistant Secretary of State for Educational and Cultural Affairs. Also at that time, Chairman Royce's House Foreign Affairs Committee was attempting to advance H.R. 2712, known as the " Hamas Sanctions Bill," which specifically named Qatar as a sponsor of Hamas subject to sanctions. It was only one of a series of articles hostile to Broidy authored by Wieder following contact with Muzin and Howard, who also had extensive communications with Wieder's editor, Viveca Novak.

ANSWER: Insofar as the allegations contained in Paragraph 159 purportedly refer to a McClatchy article, Defendants refer to that article for its content. Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations contained in Paragraph 159.

160. And on May 4, 2018, in a WhatsApp message to Allaham, Muzin summed up the very obvious objective the Enterprise had pursued for months, stating: "our new friends can make Broidy go away altogether."

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 160, except that they deny any allegation contained in Paragraph 160 directed at them.

161. Media outlets in the United States and abroad threatened to publish—and continued to publish—materials stolen from Plaintiffs well into 2019.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 161.

162. GRA's extensive hacking and packaging of curated PDFs with hacked materials,

as well as its intentional coordination with public relations professionals, ensured that the Enterprise inflicted maximum damage on Broidy and BCM.

ANSWER: Defendants deny the allegations contained in Paragraph 162.

ii. Misleading and Malicious News Articles based on the Stolen Materials Damage Plaintiffs.

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

163. As an example, one news article using the hacked materials appeared on March 1, 2018, in *The Wall Street Journal*, and was titled “Trump Ally Was in Talks to Earn Millions in Effort to End 1MDB Probe in U.S. Emails indicate Republican donor and wife were negotiating fee if the Justice Department closed its investigation.”

ANSWER: Insofar as Paragraph 163 purports to set forth an “example” of the allegations contained in Paragraph 162, Defendants refer to, and incorporate here, their response to Paragraph 162. The allegations contained in Paragraph 163 purportedly refer to a Wall Street Journal article. Defendants refer to that article for its content.

164. A deluge of articles followed, as demonstrated by these examples:

- a. 3/2/18 – *Huffington Post*, “Leaked Emails Appear to Show a Top Trump Fundraiser Abusing His Power”
- b. 3/3/18 – *The New York Times*, “Mueller’s Focus on Adviser to Emirates Suggests Broader . . .”
- c. 3/5/18 – *BBC News*, “Emails Show UAE-Linked Effort Against Tillerson”
- d. 3/5/18 – *The New York Times*, “A Top Trump Fund-Raiser Says Qatar Hacked His Email”
- e. 3/6/18 – *Bloomberg*, “Trump Fundraiser’s Email Breach Shows Risks Before Midterms”

- f. 3/9/18 – *Huffington Post*, “Leaked Memo”
- g. 3/12/18 – *Hollywood Reporter*, “Mueller Probe Expands to Hollywood as Trump Arrives . . .”
- h. 3/21/18 – *The New York Times*, “How 2 Gulf Monarchies Sought to Influence the White House”
- i. 3/23/18 – *Bloomberg*, “Trump Fundraiser Offered to Help Lift Sanctions on Russian Firms”
- j. 3/29/18 – *Newsweek*, “Top Trump Fundraiser Helped Congressman’s Wife Land State Department Job”

ANSWER: The allegations contained in Paragraph 164 purportedly refer to a number of articles. Defendants refer to those articles for their contents, and state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the remaining allegations in that paragraph.

165. The *Huffington Post*’s March 2, 2018 article expressly stated that it was based on “[e]mails and documents an anonymous group leaked.” The same article also included a screenshot of what purported to be a leaked email.

ANSWER: The allegations contained in Paragraph 165 purportedly refer to a Huffington Post article. Defendants refer to that article for its content and the characterization of that content.

166. Similarly, the *BBC News* article from March 5, 2018 admitted that “BBC has obtained leaked emails” from Broidy.

ANSWER: The allegations contained in Paragraph 166 purportedly refer to a BBC article. Defendants refer to that article for its content.

167. Additionally, *The New York Times* article from March 5, 2018 made assertions based on “three sets of documents that appear to have been hacked from Broidy’s personal email.”

ANSWER: The allegations contained in Paragraph 167 purportedly refer to a N.Y. Times article. Defendants refer to that article for its content.

G. Although the Hack-and-Smear Campaign Did Not Silence Broidy, It Caused Broidy and BCM to Suffer Significant Harm and Business Losses.

ANSWER: No response is required to the headings set forth in the SAC. Insofar as a response is deemed necessary, Defendants deny any allegations in the headings that are directed at them.

168. The hack-and-smear campaign by GRA and Chalker did not accomplish its primary objective of silencing Broidy, whose opposition to Qatar's support for terrorism is now stronger than ever.

ANSWER: Defendants deny the allegations contained in Paragraph 168.

169. Nonetheless, the unlawful and tortious conduct of GRA and Chalker has caused Broidy and BCM to suffer significant economic losses in the form of lost business relationships and lost contracts.

ANSWER: Defendants deny the allegations contained in Paragraph 169.

170. For example, BCM lost out on contract opportunities with at least two foreign governments as a direct result of the hacked materials being disseminated.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 170, except that they deny any involvement in the alleged hack-and-smear operation.

171. Broidy personally has been damaged in his broader business affairs, as business partners and others have not wanted to associate themselves with someone who, following the press onslaught, had such high visibility as a result of being the subject of deceptive, unflattering media coverage. For example, investment and commercial banks with whom Broidy had long-

term relationships suddenly ceased doing business with him, following the hacks and associated media campaign. BCM had at least one financial institution that also ceased doing business with BCM as a direct result of the hacked materials being disseminated.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 171, except that they deny any involvement in the alleged hack-and-smear operation.

172. One element of this harm is that BCM has lost significant revenue and goodwill. BCM makes investments in, among other things, privately held defense contracting companies. In the defense contracting space, discretion is very important and highly valued. The projects of BCM portfolio companies involve sensitive counterterrorism and intelligence initiatives. The work is both highly confidential and proprietary. BCM clients rely on the company to protect information that is highly sensitive, and the fact that BCM was hacked—and that the fruits of the hack were spread through the media—has, quite predictably, caused counterparties and others to flee, and resulted in a substantial loss in business.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 172, except that they deny any involvement in the alleged hack-and-smear operation.

173. In addition to the harmful effects on Plaintiffs' business, BCM and Broidy also incurred significant losses in the form of investigating the hacks, repairing the damage to BCM's systems caused by the hacks, updating the security protocols, and installing the necessary protections to prevent GRA and Chalker from committing similar hacks in the future. These costs, which were directly caused by the hacking, amounted to hundreds of thousands of dollars paid out by Broidy and BCM.

ANSWER: Defendants state that they lack knowledge or information sufficient to form a belief as to the truth or falsity of the allegations contained in Paragraph 173, except that they deny any involvement in the alleged hack-and-smear operation and any other allegations contained in Paragraph 173 directed at Defendants GRA and Chalker.

**CLAIM I
Violation of the Stored Communications Act, 18 U.S.C. § 2701, et seq.
(GRA and Chalker)²²**

174. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

ANSWER: Defendants GRA and Chalker incorporate their answers to each of the referenced paragraphs as though set forth here in full.

175. The Stored Communications Act (“SCA”) imposes criminal penalties on “whoever . . . intentionally accesses without authorization a facility through which an electronic communication service is provided. . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system” 18 U.S.C. § 2701(a).

ANSWER: Paragraph 175 purports to set forth the requirements of the Stored Communications Act (“SCA”). Defendants GRA and Chalker refer to the SCA for its contents.

176. The SCA also provides that “a person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity” damages, along with equitable

22. Plaintiffs assert Claim I against Defendants GRA and Chalker only. Because this claim is not directed at Defendants Mandich and Garcia, no responsive pleading is required from them for the allegations set forth under this claim. Insofar as any such allegations are directed at them, they deny those allegations.

and declaratory relief. *Id.* § 2707.

ANSWER: Paragraph 176 purports to set forth the requirements of the SCA. Defendants GRA and Chalker refer to the SCA for its contents.

177. Broidy and BCM are “persons” within the meaning of 18 U.S.C. §§ 2510(6) and 2707(a).

ANSWER: Paragraph 177 contains legal conclusions to which no response is required.

178. GRA and Chalker are directly liable under the SCA because they directed and controlled the hacking of Plaintiffs’ email servers, facilities, and computer systems.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 178.

179. GRA and Chalker willfully, flagrantly, and intentionally accessed without authorization a facility through which an electronic communication service is provided, namely, BCM’s computer systems, including its email servers, as well as Google’s servers, thereby obtaining access to wire or electronic communications while they were in electronic storage in such systems, in violation of 18 U.S.C. § 2701(a).

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 179.

180. The cyberattack was a willful, flagrant, and intentional violation of the SCA.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 180.

181. GRA and Chalker willfully and intentionally accessed the email accounts of, at a minimum, Broidy, Caganap, Hilliard, Rosenzweig, Levi, Sexton, and Stephens by transmitting fake spear phishing emails with links to malicious websites enabling GRA and Chalker to steal

the login credentials.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 181.

182. GRA and Chalker used the information they obtained from their spear phishing attacks to gain unauthorized access to Plaintiffs' computer networks and email accounts. Beginning on or about January 16, 2018, Defendants intentionally accessed or caused to be accessed BCM's servers without authorization, including emails and documents physically located on those servers, as well as Google servers, specifically by accessing, or causing others to access, the accounts of Broidy and other BCM employees, without authorization and obtaining emails and other items.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 182.

183. GRA and Chalker also implemented identifiable obfuscation techniques, such as VPN, to engage in efforts to hide the origin of their spear phishing attacks and unauthorized access to Plaintiffs' servers, and emails and documents physically located on those servers and the servers of Google. GRA and Chalker used VPN and other tools to mask their cyber intrusions and avoid detection, thereby showing sophistication and consciousness of guilt.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 183.

184. GRA and Chalker intentionally, willfully, unlawfully, and without authorization accessed Plaintiffs' computer systems and email servers thousands of times over a period of almost two months, in a sustained cyberattack.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 184.

185. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

- (a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;
- (b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;
- (c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;
- (d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;
- (e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and
- (f) additional harm and damages to be proven at trial.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 185.

186. GRA and Chalker intentionally and willfully caused such damage to Plaintiffs.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 186.

187. The total amount of these losses will be proven at trial but, in any event, far exceeds \$75,000. In fact, the out-of-pocket costs Plaintiffs paid to outside consultants to conduct a damage assessment and for remedial measures was alone in the hundreds of thousands of dollars.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 187.

188. As provided for in 18 U.S.C. § 2707(b) & (c), Plaintiffs are entitled to an award of the greater of the actual damages suffered or the statutory damages, as well as punitive damages, attorneys' fees and other costs of this action, and appropriate equitable relief.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 188.

CLAIM II
Violation of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030(a)(2) and (a)(5) (All Defendants)²³

189. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

ANSWER: Defendants incorporate their answers to each of the referenced paragraphs as though set forth here in full.

190. The Computer Fraud and Abuse Act ("CFAA") creates a cause of action against whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2).

23. Pursuant to the Motion to Dismiss Order, GRA EMEA, GRA Maven, GRA Quantum, GRA Research, Qrypt, and Courtney Chalker are no longer parties to this action. Insofar as Plaintiffs direct the allegations in Claim II at those former defendants, no response is required.

ANSWER: Paragraph 190 purports to set forth certain provisions of the Computer Fraud and Abuse Act (“CFAA”). Defendants refer to the CFAA for its contents.

191. The CFAA also creates a cause of action against whoever “(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.” *Id.* § 1030(a)(5).

ANSWER: Paragraph 191 purports to set forth certain provisions of the CFAA. Defendants refer to the CFAA for its contents.

192. The CFAA also creates a cause of action against “[w]hoever conspires to commit or attempts to commit an offense under subsection (a) of this section.” *Id.* § 1030(b).

ANSWER: Paragraph 192 purports to set forth certain provisions of the CFAA. Defendants refer to the CFAA for its contents.

193. A “protected computer” is one that “is used in or affecting interstate or foreign commerce or communication.” *Id.* § 1030(e)(2)(B).

ANSWER: Paragraph 193 purports to set forth certain provisions of the CFAA. Defendants refer to the CFAA for its contents.

194. BCM’s computer systems and email servers are used in and affect interstate and foreign commerce or communication and are therefore “protected computers.”

ANSWER: Paragraph 194 contains legal conclusions to which no response is required.

195. GRA and Chalker willfully and intentionally accessed the email accounts of, at a minimum, Broidy, Caganap, Hilliard, Rosenzweig, Levi, Sexton, and Stephens by transmitting

fake spear phishing emails with links to malicious websites enabling GRA and Chalker to steal the login credentials.

ANSWER: Defendants deny the allegations contained in Paragraph 195.

196. GRA and Chalker are directly liable under the CFAA because they directed and controlled the hacking of Plaintiffs' email servers, facilities, and computer systems.

ANSWER: Defendants deny the allegations contained in Paragraph 196.

197. GRA and Chalker willfully and intentionally accessed Plaintiffs' computer networks and email accounts without authorization.

ANSWER: Defendants deny the allegations contained in Paragraph 197.

198. Thereafter, GRA and Chalker used the information they obtained from their spear phishing attacks to gain unauthorized access to Plaintiffs' computer networks and email accounts. Beginning on or about January 16, 2018, GRA and Chalker intentionally accessed or caused to be accessed BCM's servers without authorization, including emails and documents physically located on those servers, as well as Google servers, specifically by accessing, or causing others to access, the accounts of Broidy and other BCM employees, without authorization.

ANSWER: Defendants deny the allegations contained in Paragraph 198.

199. GRA and Chalker also implemented identifiable obfuscation techniques, such as VPN, to engage in efforts to hide the origin of their spear phishing attacks and unauthorized access to Plaintiffs' servers, and emails and documents physically located on those servers and the servers of Google. GRA and Chalker used VPN and other tools to mask their cyber intrusions and avoid detection, thereby showing sophistication and consciousness of guilt.

ANSWER: Defendants deny the allegations contained in Paragraph 199.

200. GRA and Chalker intentionally, willfully, unlawfully, and without authorization accessed Plaintiffs' protected computer systems and email servers thousands of times over a period of almost two months, in a sustained cyberattack.

ANSWER: Defendants deny the allegations contained in Paragraph 200.

201. Defendants intentionally conspired to cause damage to BCM's protected computers through the attack.

ANSWER: Defendants deny the allegations contained in Paragraph 201.

202. They knowingly caused the transmission of a program, information, code, or command, and as a result, intentionally caused damage without authorization, to BCM's protected computers.

ANSWER: Defendants deny the allegations contained in Paragraph 202.

203. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

- (a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;
- (b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;
- (c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;
- (d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of

media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;

- (e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and
- (f) additional harm and damages to be proven at trial.

ANSWER: Defendants deny the allegations contained in Paragraph 203.

204. The total amount of these losses will be proven at trial but, in any event, far exceeds \$75,000. In fact, the out-of-pocket costs Plaintiffs paid to outside consultants to conduct a damage assessment and for remedial measures was alone in the hundreds of thousands of dollars.

ANSWER: Defendants deny the allegations contained in Paragraph 204.

205. GRA and Chalker intentionally and willfully caused such damage to Plaintiffs.

ANSWER: Defendants deny the allegations contained in Paragraph 205.

CLAIM III

Violation of CA Comprehensive Computer Data Access & Fraud Act, Cal. Pen. Code § 502 (GRA and Chalker)²⁴

206. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

ANSWER: Defendants GRA and Chalker incorporate their answers to each of the referenced paragraphs as though set forth here in full.

207. The California Comprehensive Computer Data Access and Fraud Act ("CDAFA") law imposes criminal penalties on anyone who "[k]nowingly accesses and without

24. Plaintiffs assert Claim III against Defendants GRA and Chalker only. Because this claim is not directed at Defendants Mandich and Garcia, no responsive pleading is required from them for the allegations set forth under this claim. Insofar as any such allegations are directed at them, they deny those allegations.

permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.” Cal. Penal Code § 502(c)(2).

ANSWER: Paragraph 207 purports to set forth certain provisions of the California Comprehensive Computer Data Access and Fraud Act (“CDAFA”). Defendants GRA and Chalker refer to the CDAFA for its contents.

208. CDAFA imposes criminal penalties on anyone who “[k]nowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.” *Id.* § 502(c)(4).

ANSWER: Paragraph 208 purports to set forth certain provisions of the CDAFA. Defendants GRA and Chalker refer to the CDAFA for its contents.

209. CDAFA imposes criminal penalties on anyone who “[k]nowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of” Section 502. *Id.* § 502(c)(6).

ANSWER: Paragraph 209 purports to set forth certain provisions of the CDAFA. Defendants GRA and Chalker refer to the CDAFA for its contents.

210. CDAFA imposes criminal penalties on anyone who “[k]nowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.” *Id.* § 502(c)(7).

ANSWER: Paragraph 210 purports to set forth certain provisions of the CDAFA. Defendants GRA and Chalker refer to the CDAFA for its contents.

211. CDAFA imposes criminal penalties on anyone who “[k]nowingly and without permission uses the Internet domain name or profile of another individual, corporation, or entity in connection with the sending of one or more electronic mail messages or posts and thereby damages or causes damage to a computer, computer data, computer system, or computer network.” *Id.* § 502(c)(9).

ANSWER: Paragraph 211 purports to set forth certain provisions of the CDAFA.

Defendants GRA and Chalker refer to the CDAFA for its contents.

212. CDAFA provides that “the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief. Compensatory damages shall include any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access.” *Id.* § 502(e)(1).

ANSWER: Paragraph 212 purports to set forth certain provisions of the CDAFA.

Defendants GRA and Chalker refer to the CDAFA for its contents.

213. CDAFA provides for award of reasonable attorneys’ fees. *Id.* § 502(e)(2).

ANSWER: Paragraph 213 purports to refer to the CDAFA. Defendants GRA and Chalker refer to that statute for its contents.

214. GRA and Chalker are directly liable under CDAFA because they directed and controlled the hacking of Plaintiffs’ email servers, facilities, and computer systems.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 214.

215. GRA and Chalker knowingly and unlawfully accessed computers, computer systems or computer networks at Plaintiff BCM and Google, all of which were located in California. GRA and Chalker knew at the time that they did not have the authorization to access Plaintiffs' computers, computer systems, and networks. This knowledge is demonstrated by their use of spear phishing attacks and attempted spear phishing attacks to disguise their intentions and obtain login credentials through fraudulent misrepresentations. The spear phishing emails imitated Google's profile in order to obtain login credentials. GRA and Chalker caused damage to Plaintiffs' electronic files and emails through their cyber intrusions.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 215.

216. GRA and Chalker knowingly and unlawfully conducted the hacking of BCM's computer systems and email servers, and are therefore directly liable under CDAFA.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 216.

217. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

- (a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;
- (b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;
- (c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks; and

- (d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;
- (e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and
- (f) additional harm and damages to be proven at trial.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 217.

218. The total amount of these losses will be proven at trial but, in any event, far exceeds \$75,000. In fact, the out-of-pocket costs Plaintiffs paid to outside consultants to conduct a damage assessment and for remedial measures was alone in the hundreds of thousands of dollars. These losses include significant costs that were reasonably necessary to verify whether and how Plaintiff's computer systems and data were altered, damaged or deleted by GRA and Chalker's unlawful access.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 218.

219. GRA and Chalker's actions were willful and malicious, and Plaintiffs are entitled to punitive damages under § 502(e)(4).

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 219.

CLAIM IV
Receipt and Possession of Stolen Property in Violation of Cal. Penal Code § 496
(All Defendants)²⁵

220. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

ANSWER: Defendants incorporate their answers to each of the referenced paragraphs as though set forth here in full.

221. California law imposes criminal penalties on any “person who buys or receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling or withholding any property from the owner, knowing the property to be so stolen or obtained.” Cal. Penal Code § 496(a).

ANSWER: Paragraph 221 purports to set forth certain provisions of the California Penal Code. Defendants GRA and Chalker refer to the California Penal Code for its contents.

222. California law further provides that “[a]ny person who has been injured by a violation of [Section 496] may bring an action for three times the amount of actual damages, if any, sustained by plaintiff, costs of suit, and reasonable attorney’s fees.”

ANSWER: Paragraph 222 purports to set forth certain provisions of the California Penal Code. Defendants GRA and Chalker refer to the California Penal Code for its contents.

223. GRA and Chalker are directly liable because they directed and controlled the hacking of Plaintiffs’ email servers, facilities, and computer systems located in California.

ANSWER: Defendants deny the allegations contained in Paragraph 223.

25. Pursuant to the Motion to Dismiss Order, GRA EMEA, GRA Maven, GRA Quantum, GRA Research, Qrypt, and Courtney Chalker are no longer parties to this action. Insofar as Plaintiffs direct the allegations in Claim IV at those former Defendants, no response is required.

224. GRA and Chalker knowingly received property, including private communications, documents, trade secrets and intellectual property housed on Plaintiffs' and Google's servers, and in emails and documents physically located on those servers located in California.

ANSWER: Defendants deny the allegations contained in Paragraph 224.

225. This property was stolen from Plaintiffs in California or otherwise obtained from Plaintiffs in California in a manner that constitutes theft.

ANSWER: Defendants deny the allegations contained in Paragraph 225.

226. GRA and Chalker received the property knowing that it was stolen property and obtained through theft. They knowingly and intentionally concealed, sold, withheld—and aided in the concealing, selling and withholding—of Plaintiffs' stolen property.

ANSWER: Defendants deny the allegations contained in Paragraph 226.

227. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

- (a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;
- (b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;
- (c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;
- (d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial

measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;

- (e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and
- (f) additional harm and damages to be proven at trial.

ANSWER: Defendants deny the allegations contained in Paragraph 227.

228. The total amount of these losses will be proven at trial but, in any event, far exceeds \$75,000.

ANSWER: Defendants deny the allegations contained in Paragraph 228.

CLAIM V
Intrusion Upon Seclusion (GRA and Chalker)²⁶

229. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

ANSWER: Defendants GRA and Chalker incorporate their answers to each of the referenced paragraphs as though set forth here in full.

230. Plaintiffs have a legally protected privacy interest in their information. This includes their Google login information, their emails, and documents contained on BCM's servers and computer systems. Plaintiffs' email servers and computer systems contained private information and secrets that Plaintiffs had secluded away from public attention and prying eyes.

ANSWER: Paragraph 230 contains legal conclusions to which no response is required.

231. GRA and Chalker are directly liable under CDAFA because they directed and

26. Plaintiffs assert Claim V against Defendants GRA and Chalker only. Because this claim is not directed at Defendants Mandich and Garcia, no responsive pleading is required from them for the allegations set forth under this claim. Insofar as any such allegations are directed at them, they deny those allegations.

controlled the hacking of Plaintiffs' email servers, facilities, and computer systems.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 231.

232. GRA and Chalker purposefully and repeatedly hacked Plaintiffs' computer systems and email servers over a period of weeks. In doing so, they intruded upon Plaintiffs' secluded documents and private communications, viewing them through electronic means and then printing them out.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 232.

233. Much of the information GRA and Chalker illegally obtained in the hacking concerned Broidy's private matters and is not of public interest. GRA and Chalker's tortious scheme—committing repeated cybercrimes to facilitate the publishing of a private citizen's secrets—is highly offensive and shocking to any reasonable person. GRA and Chalker were retained specifically as part of an effort to harm Broidy's business and public standing. They accomplished that end through illegal means, by stealing and conspiring to publish private facts about his personal life and matters.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 233.

234. GRA and Chalker intruded upon Broidy's seclusion between January 16, 2018 and February 25, 2018 and other times within two years of the commencement of this action.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 234.

235. The stealing and subsequent public disclosure of misleading and curated

information has caused Plaintiffs to suffer monetary damages, in an amount to be proven at trial, but in any event, in excess of \$75,000, exclusive of interest and costs. The injury to Plaintiffs' privacy is ongoing, and thus the damages Plaintiffs seek may not be finally set. Because GRA and Chalker's actions are intolerable in a civilized community, Plaintiffs also seek punitive damages to deter this sort of criminal enterprise behavior.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 235.

236. As a direct and proximate result of the actions of GRA and Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

- (a) harm to Plaintiffs' computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;
- (b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs' servers, systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;
- (c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;
- (d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;
- (e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and
- (f) additional harm and damages to be proven at trial.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 236.

237. The total amount of these losses will be proven at trial but, in any event, far exceeds \$75,000.

ANSWER: Defendants GRA and Chalker deny the allegations contained in Paragraph 237.

CLAIM VI
Civil Conspiracy (All Defendants)²⁷

238. Plaintiffs incorporate and adopt by reference the allegations contained in each and every preceding paragraph.

ANSWER: Defendants incorporate their answers to each of the referenced paragraphs as though set forth here in full.

239. GRA, Kevin Chalker, Mandich, Garcia, and Courtney Chalker formed and operated a conspiracy.

ANSWER: Defendants deny the allegations contained in Paragraph 239.

240. Defendants willfully, intentionally, and knowingly agreed to violate the SCA, the CFAA, and CDAFA, to receive and possess stolen property, and to intrude upon Broidy's seclusion, all as further described above and incorporated herein. Defendants operated their conspiracy to accomplish these ends.

ANSWER: Defendants deny the allegations contained in Paragraph 240.

241. GRA and Chalker willfully, intentionally, and knowingly directed and controlled

27. Pursuant to the Motion to Dismiss Order, GRA EMEA, GRA Maven, GRA Quantum, GRA Research, Qrypt, and Courtney Chalker are no longer parties to this action. Insofar as Plaintiffs direct the allegations in Claim VI at those former Defendants, no response is required.

the illegal acts, as described above.

ANSWER: Defendants deny the allegations contained in Paragraph 241.

242. Mandich furthered the illegal acts by willfully, intentionally, and knowingly designing and strategizing the “special projects” including covert operations at Chalker’s direction.

ANSWER: Defendants deny the allegations contained in Paragraph 242.

243. Garcia and Courtney Chalker furthered the illegal acts by willfully, intentionally, and knowingly destroying evidence of the conspiracy’s unlawful and tortious conduct at Chalker’s direction. Defendants wiped GRA’s computers, phones and other devices clean of any damaging evidence; removed certain hard drives, phones and devices with incriminating evidence from GRA’s offices’ and brought those devices to a remote location where Defendants destroyed them.

ANSWER: Defendants deny the allegations contained in Paragraph 243.

244. Each of the Defendants actively participated in the above-described civil conspiracy, and therefore each Defendant is responsible for each tortious and otherwise unlawful action of any co-conspirator.

ANSWER: Defendants deny the allegations contained in Paragraph 244.

245. As a direct and proximate result of the conspiracy, including the conduct of Mandich, Garcia, and Courtney Chalker, Plaintiffs incurred substantial losses and damage, including but not limited to:

- (a) harm to Plaintiffs’ computers, servers and accounts, including the integrity and availability of their servers, and to emails and documents physically located on those servers;
- (b) losses associated with identifying and investigating the cyberattacks, and assessing and repairing the integrity and security of Plaintiffs’ servers,

systems and operations after the attacks, including the costs of hiring forensic investigators, data security experts, and attorneys;

- (c) losses associated with remedial measures taken to prevent future attacks, including but not limited to the replacement costs for personal and business computers and cell phones, and consultant fees to reprogram Plaintiffs' new computer and cell phone equipment to create dual authentication systems, in order to help prevent future attacks;
- (d) harm to Plaintiffs' business, including but not limited to lost revenue from business arrangements cancelled or lost due to the hack and associated media onslaught, losses associated with hundreds of hours of Broidy's and other employees' time spent investigating the hacking, taking remedial measures in response to the hacking, and responding to the barrage of media inquiries, rather than time spent on billable business matters, as well as loss of goodwill;
- (e) loss in the value of Plaintiffs' trade secrets, confidential and proprietary business information, and other intellectual property, and losses associated with protecting the foregoing from future misappropriation; and
- (f) additional harm and damages to be proven at trial.

ANSWER: Defendants deny the allegations contained in Paragraph 245.

246. The total amount of these losses will be proven at trial but, in any event, far exceeds \$75,000.

ANSWER: Defendants deny the allegations contained in Paragraph 246.

CLAIM VII
Violation of the Defend Trade Secrets Act, 18 U.S.C. §§ 1831, 1832, 1836
(All Defendants)

This cause of action, alleged in Paragraphs 247 through 269 of the SAC has been dismissed by the Motion to Dismiss Order, and no responsive pleading is required. If a response is deemed required, the allegations in said paragraphs are denied.

CLAIM VIII
Violation of the California Uniform Trade Secrets Act, Cal. Civ. Code § 3426
(GRA and Chalker)

This cause of action, alleged in Paragraphs 270 through 283 of the SAC, has been dismissed by the Motion to Dismiss Order, and no responsive pleading is required. If a response is deemed required, the allegations in said paragraphs are denied.

CLAIM IX
Violation of the RICO Act, 18 U.S.C. §§ 1962(c) and 1964
(All Defendants)

This cause of action, alleged in Paragraphs 284 through 341 of the SAC, has been dismissed by the Motion to Dismiss Order, and no responsive pleading is required. If a response is deemed required, the allegations in said paragraphs are denied.

CLAIM X
Conspiracy to Violate the RICO Act, 18 U.S.C. § 1962(d)
(All Defendants)

This cause of action, alleged in Paragraphs 342 through 350 of the SAC, has been dismissed by the Motion to Dismiss Order, and no responsive pleading is required. If a response is deemed required, the allegations in said paragraphs are denied.

GENERAL DENIAL

Defendants deny all allegations in the SAC not specifically admitted herein.

RESPONSE TO PRAYER FOR RELIEF

Defendants deny that Plaintiffs have any basis for any relief they seek against them.

AFFIRMATIVE DEFENSES

Defendants assert the following affirmative defenses to the claims alleged in the SAC. In doing so, Defendants do not assume the burden of proof with respect to any fact or proposition necessary to any of the following defenses where the burden is legally and properly imposed on Plaintiffs. Defendants set forth these defenses without waiving any other applicable defenses, affirmative or otherwise.

The allegations in the SAC are vague and conclusory and rely heavily on unidentified sources. Defendants are therefore not able to consider and raise all appropriate defenses at this time. Defendants are continuing to investigate Plaintiffs' claims and have insufficient knowledge or information on which to form a belief as to whether there may be additional affirmative defenses available to them. Accordingly, Defendants expressly reserve the right to raise additional affirmative defenses as they become known to them.

1. The SAC fails to state a claim upon which relief may be granted to Plaintiffs against any Defendant.

2. Certain acts or omissions attributed to one or more Defendants in the SAC relate to national security information classified under Executive Order 13526, (Dec. 29, 2009), information which is the property of the United States, the unauthorized disclosure of which could cause irreparable injury to the United States or be used to advantage by foreign nations. Defendants are bound by executed Classified Information Nondisclosure Agreements to receive prior written notice of authorization from the United States Government Department or Agency responsible for the classification of this information that any such disclosure in this Answer is permitted. The unauthorized disclosure of this information might constitute violations of 18 U.S.C. §§ 641, 793, 794, 798, 952 and 1924, 50 U.S.C. § 783, and/or the Intelligence Identities Protection Act of 1982. (*See* Standard Form 312.) However, no such alleged acts or omissions relate to Plaintiffs' alleged hack-and-smear allegations in any way.

3. The claims asserted in the SAC against Defendants are barred, in whole or in part, because any damage allegedly suffered by Plaintiffs was not caused by any action attributable to any Defendant.

4. No Defendant is responsible in any way for the acts or omissions of any persons who caused the damages that Plaintiffs allege they suffered (if any).

5. The claims asserted in the SAC against Defendants are barred because the instant suit is meritless and brought in bad faith.

6. Plaintiffs engaged in inequitable conduct directly related to the claims asserted in the SAC. Plaintiffs' claims are therefore barred by the doctrine of unclean hands.

7. The claims asserted in the SAC against Defendants are barred because Plaintiffs lack standing to assert them.

8. The claims asserted in the SAC against Defendants are barred by the applicable statutes of limitations.

9. The SAC, and each cause of action presented therein, fails to state facts constituting a claim for which punitive damages may be awarded against Defendants.

10. Insofar as the SAC seeks punitive damages, it violates Defendants' procedural and substantive due process rights.

11. Plaintiffs' claims are barred, in whole or in part, by the doctrines of laches, waiver and estoppel.

12. The claims asserted in the SAC against Defendants are barred, in whole or in part, because Plaintiffs failed to make reasonable efforts to mitigate any alleged injury or damage.

13. The claims asserted in the SAC against Defendants are barred, in whole or in part, because the alleged damages are too speculative and uncertain, and because of the impossibility of ascertaining and allocating the alleged damages.

14. Plaintiffs are not entitled to recover attorneys' fees, experts' fees, or any other costs and disbursements in this action.

RESPONSE TO DEMAND FOR JURY TRIAL

Defendants object to Plaintiffs' demand for jury trial to the extent any of Plaintiffs' claims or underlying issues are not triable by a jury.

Dated: New York, New York
October 12, 2023

HUGHES HUBBARD & REED LLP

By: /s/ Marc A. Weinstein

Marc A. Weinstein
Kevin T. Carroll
Amina Hassan

One Battery Park Plaza
New York, New York 10004-1482
Telephone: (212) 837-6000
Fax: (212) 422-4726
marc.weinstein@hugheshubbard.com
kevin.carroll@hugheshubbard.com
amina.hassan@hugheshubbard.com

Attorneys for Defendants